TARTU ÜLIKOOL

MATEMAATIKA-INFORMAATIKATEADUSKOND

Arvutiteaduse instituut

Infotehnoloogia eriala

Eveli Pung

TOIMEPIDEVUSE TAGAMINE JA KORRALDUS AVALIKE TEENUSTE OSUTAMISEL EESTIS

Magistritöö (30 EAP)

Juhendaja: Erkki Leego

Autor: …… „…..“ jaanuar 2012

Juhendaja: ……. „…..“ jaanuar 2012

Lubada kaitsmisele

Professor ……..…….. „…..“ jaanuar 2012

Tartu 2012

SISUKORD

SISSEJUHATUS

Toimepidevus ehk talitluspidevus on protsesside järjepideva toimimise suutlikkus ja taastamise võime pärast katkestust [1]. Protsesside all mõistetakse enamasti kahte liiki tegevusi - teenuse osutamist või toote valmistamist. Toimepidevuse tagamisel on eesmärgiks, et ettevõte või asutus oleks kindlustatud erinevate riskide vastu ja saaks katkestuse korral võimalikult kiiresti oma põhitegevust jätkata.

Toimepidevuse tagamine on sisuliselt elementaarne kontseptsioon, mida on vähemal või suuremal määral rakendatud aastasadu. Juba keskaja rätsep tegeles toimepidevuse tagamisega hankides tagavarakäärid. Praegu on aga kätte jõudnud ajastu, kus protsessid ja neid toetavad süsteemid on muutunud oluliselt keerulisemaks. Seetõttu on toimepidevuse tagamine tänapäevases infoühiskonna võtmes võrdlemisi uus kontseptsioon. Paljud ettevõtted ja asutused on teatud määral tegelenud riskide maandamisega ning jätkusuutlikkuse aspektid igapäevatöö raames läbi mõelnud, kuid toimepidevusplaanide koostamine on uus distsipliin, mille teadvustamine ja rakendamine võtab veel aega.

Antud magistritöö eesmärkideks on:

1. Tõsta toimepidevusealast teadlikkust.
2. Anda ülevaade toimepidevuse tagamise taustast Eestis ja maailmas.
3. Konkreetselt ja arusaadavalt lahti seletada toimepidevuse tagamiseks vajalikud tegevused.
4. Pakkuda täiendavat materjali eestikeelsetele toimepidevuse alastele juhenditele.
5. Saada ülevaade Eesti avalike teenuste toimepidevuse olukorrast.
6. Identifitseerida kitsaskohad ja teha saadud ülevaate põhjal ettepanekuid toimepidevuse tagamise edendamiseks.

Magistritöö on jaotatud kaheks loogiliseks osaks – toimepidevuse tagamise teooria ja ülevaade Eesti avalike teenuste toimepidevusest. Töö rõhuasetus on eelkõige IT-alasel toimepidevusel.

Esimeses peatükis kirjeldatakse toimepidevuse tagamise tausta Eestis ja maailmas. Antakse ülevaade arengutest viimaste aastakümnete jooksul, analüüsitakse valdkonnaga seotud statistikat ja tuuakse välja vastavad standardid ja juhendid.

Teine peatükk on pühendatud toimepidevuse tagamise teooriale. Kirjeldatakse ärimõju analüüsi ja riskianalüüsi läbiviimist, riskide maandamist, toimepidevusplaani koostamist, testimist ja hooldust. Samuti tuuakse välja toimepidevuse eelarve ja meeskonna koostamise põhimõtted ning soovitused kriisikommunikatsiooni korraldamiseks.

Kolmandas peatükis analüüsitakse Eesti avalike teenuste toimepidevust. Viiakse läbi intervjuud erinevate osapooltega – infosüsteemide kolmeastmeline etalonturbe süsteemi ISKE rakendajatega, ISKE koordineerijatega riiklikul tasandil, elutähtsate teenuste osutajatega, neid korraldavate asutustega ja seadusandluse algatajatega. Kogutud informatsiooni põhjal koostatakse ülevaade ISKE-ga reguleeritud avalike teenuste ja hädaolukorra seaduse alusel opereerivate elutähtsate teenuste toimepidevuse kohta.

Neljandas peatükis esitatakse valminud ülevaadete põhjal peamised tähelepanekud ja järeldused Eesti avalike teenuste toimepidevuse korralduse kohta.

Viiendas peatükis tehakse valminud ülevaate, tähelepanekute, järelduste, avalike dokumentide ja ülejäänud informatsiooniallikate põhjal ettepanekud toimepidevuse tagamise edendamiseks.

Magistritöö lisades on ära toodud intervjuude läbiviimisel autori poolt esitatud küsimused.

1 TOIMEPIDEVUSE TAGAMISE ÜLEVAADE EESTIS JA MAAILMAS

Toimepidevuse tagamisest hakati esmakordselt rääkima 1980. aastatel. Avaldati raamatuid ja artikleid katastroofijärgse taastamise kohta ning tööle hakkasid esimesed talitluspidevuse tagamisele suunatud organisatsioonid [2]. Murdepunktiks sai 2001. aasta terrorirünnak USA-s, mis paljastas nõrkused olemasolevates talitluspidevusplaanides ning mille järel hakati oluliselt rohkem tähelepanu pöörama IT infrastruktuuri kaitsele [3]. Samuti olid olulisteks sündmusteks 2004 ja 2005. aasta orkaanid USA-s ja terrorirünnakud Euroopas, mille mõjutusel sai alguse Euroopa kriitilise infrastruktuuri kaitse programm EPCIP (European Programme for Critical Infrastructure Protection), mis keskendub elutähtsate valdkondade toimepidevuse ja kaitse tagamisele [4].

Viimaste aastate jooksul on toimunud mitmeid intsidente, mis näitavad, kui haavatavad on tänapäevased tehnoloogilistel lahendustel põhinevad protsessid. Siinkohal võib näiteks tuua 2008. aasta alguses toimunud kriisi, kus veealuste kaablite katkemise tagajärjel jäid mitmed Lähis-Ida riigid 10 päevaks Internetita ja sellest olid häiritud 80 miljonit kasutajat. [5]. Looduskatastroofide ja inimvigade kõrval on aina tõsisemaks muutunud sihilikud rünnakud. Juunis 2010 avastati Stuxneti viirus, mis suudab kahjustada Siemensi tööstuslikke seadmeid ja tarkvara. Viirus tegi kahju Iraani tuumaprogrammi raames kasutatavatele seadmetele. Spekuleeritakse, et see oligi ründe eesmärk ning antud viiruse loomist koordineeriti riiklikel tasanditel [6].

Sarnaselt kogu ülejäänud maailmaga puutus Eesti laialdasemalt toimepidevuse tagamisega kokku aastatuhandevahetusel, kui selgus et olemasolevad arvutisüsteemid ei pruugi toime tulla uue aastaarvuga. Toomas Kirt ja Jaak Tepandi kirjutasid Infotehnoloogia haldusjuhtimise aastaraamatus 1998 järgmist: „Aasta 2000 on tõsine proovikivi kogu maailma ja ka Eesti infosüsteemidele, kuna üha enam kasutatakse info töötlemisel arvutustehnikat ning automatiseeritud süsteemide töö võimalik lakkamine aastatuhandevahetusel tekitaks ettevõtetele ja ühiskonnale tervikuna korvamatut kahju.” [7]

2000. aastatel sagenesid viited toimepidevuse tagamise vajadusele. Näiteks Finantsinspektsiooni 2004. aasta aastaaruandes kirjutatakse järgmist: „Arvestades järelevalvesubjektide kiiret kasvu ja üha süvenevat sõltuvust (info)tehnoloogiast, on üha olulisemaks muutumas operatsioonilise riski seire, sh elektrooniliste teenuste turvariskid ja infotehnoloogia ala talitluspidevus.” [8].

Sündmused kevadel 2007 olid esimeseks proovikiviks toimepidevuse tagamisele - Eesti oli esimene NATO riik, mis digitaalrünnaku ohvriks langes. Mitme nädala jooksul viidi läbi laiaulatuslikke DOS rünnakuid Eesti riigiasutustele ja pankadele. Antud sündmused viisid mõistmiseni, et riiklikku julgeolekut tuleb kaitsta ka kübermaastikul [9]. 2008. aastal loodi Tallinnas NATO Kooperatiivse Küberkaitse Kompetentsikeskus, mis tegeleb küberkaitse tugevdamise väljakutsetega [10].

Detsembris 2007 anti Eestis välja määrus ISKE kolmeastmelise etalonturbe rakendamiseks riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavate infosüsteemide ning nendega seotud infovaradele turvalisuse tagamiseks [11]. 2008. aastal kaardistati Eesti elutähtsate teenuste osutajad ja 2010. aasta juunist hakkasid kehtima hädaolukorraseaduse määrused, mis sätestavad vastavate teenuste osutajate kohustust koostada riskianalüüs ja toimepidevusplaan [4].

Talitluspidevuse tagamise kohta on maailmas avaldatud erinevat ja vastuolulist statistikat. Väga palju tsiteeritakse sekundaarseid allikaid ja originaaltsitaadi tuvastamine on raske. Samuti jääb selgusetuks, millise uurimistöö ja metoodika põhjal statistilisi järeldusi on tehtud. Eksisteerib mitmeid müüte, millest on saanud loosungid talitluspidevuse tagamise teenust pakkuvatele firmadele.

Tabelis 1 on esitatud mõningaid talitluspidevuse tagamisega seotud levinumaid väiteid.

Tabel 1. Enimlevinud talitluspidevuse tagamisega seotud väited [12].

Väide	Väidetav allikas
80% ettevõtetest, mida tabab suurem kriis, ei taastu sellest kunagi või sulevad uksed järgneva 18 kuu jooksul.	AXA raport (2007)
70% ettevõtetest läheb peale fundamentaalset andmekadu pankrotti	Ühendatud Kuningriigi Kaubandus ja tööstusministeeriumi raport (2004)
80% adekvaatsete talitluspidevusplaanideta organisatsioonidest, mida tabab laialdane IT kriis, lähevad pankrotti.	IBM uuring (1993)
90% ettevõtetest läheb peale fundamentaalset andmekadu pankrotti järgmise kahe aasta jooksul	Gartneri uuring (2005)
80% läbimõeldud andmekaitse ja taastamisstrateegiateta ettevõtetest lähevad kahe aasta jooksul peale suuremat kriisi pankrotti.	Ameerika Ühendriikide rahvusarhiiv

Eksperdid on üritanud eelmainitute ja paljude teiste analoogsete statistiliste väidete tõesust ja algallikaid on kontrollida, kuid enamike tsitaatide korral ei suudetud leida algtekste või konkreetset tsitaati väidetavast algallikast [12].

Mitmed talitluspidevuse juhtimise teenust pakkuvad IT-konsultatsiooni firmad tsiteerivad järgmist väidet: statistika näitab, et keskmiselt 40% ettevõtetest, millel ei ole taasteplaani, lähevad pankrotti peale tõsist kriisi nagu tulekahju, sissemurdmine, torm või sabotaaž [13, 14, 15, 16, 17]. Identset väidet tsiteerivad ka mõned teised antud valdkonna firmad, kuid 40% on asendatud 70% [18]. Ühelgi kodulehel ei ole ära toodud tsitaadi algallikat ning eelnevad näited tõestavad, et statistikat modifitseeritakse ärieesmärkide teenimiseks mistahes määral.

Nagu eelnevast selgub, on toimepidevust puudutav statistika vähene ja selle allikaid on raske tuvastada. See on ka loomulik, sest antud valdkonda puudutavatest asjaoludest ei taheta avalikult rääkida, kuna turbe olukorra teabe jagamine on juba oma olemuselt turvarisk. Peale intervjuusid Eesti avalike teenuste toimepidevuse tagamise võtmeisikutega on tekkinud tunnetus, et enamik esitatud väidetest peegeldavad üsna adekvaatselt reaalset olukorda.

Suures plaanis on ilmne, et iga ettevõtte ja asutuse huvides on tagada selle protsesside sujuv toimimine. IT osakaal on tänapäeval Eesti ettevõtete töös väga suur. 2011. aastal kasutas 96,2% ettevõtteid arvuteid ning keskmine arvutite arv ettevõttes on 19,5 [19]. Selline statistika näitab, et sõltuvus infotehnoloogiast on tugev ning infotehnoloogiliste süsteemide toimimise kaitse peab olema toimepidevuse tagamise lahutamatu põhiosa.

Talitluspidevuse tagamine on reguleeritud standarditega ISO/IEC 27001:2005 ja ISO/IEC 27002:2005. Briti Standardite Organisatsioon on avaldanud standardid BS 25999-1 ja BS 25999-2 [20]. Samuti on avaldatud standard BSI 100-4 hädaolukordade halduse kohta, mis katab endas ka kaks eelmainitud standardit [21]. Eestis rakendatud ISKE neljaastmeline etalonturbe süsteem põhineb Saksamaa Infoturbeameti (Bundesamt für Sicherheit in der Informationstechnik, BSI) poolt publitseeritaval IT etalonturbe käsiraamatul (IT Grundschutzhandbuch'il).

Talitluspidevuse tagamise juhenditest on üks tuntumaid USA Riikliku Standardite ja Tehnoloogia Instituudi poolt välja antud „Riiklike infosüsteemide toimepidevuse planeerimise juhend", mida loetakse parimaks tegevusjuhiseks ka kõigile teistele ettevõtetele [22].

Põhilised toimepidevuse tagamise juhendid Eestis on „Toimepidevuse plaani koostamise juhend" elutähtsate teenuste osutajatele [23] ja Finantsinspektsiooni juhend „Nõuded finantsjärelevalve subjekti talitluspidevuse protsessi korraldamisele" [24]. Esimene neist ei sisalda spetsiifilisi infosüsteemide toimepidevusalaseid juhiseid. Toimepidevuse valdkonnaga tutvumisel võib abiks olla ka Riigi Infosüsteemi Ameti poolt koostatud konkreetne ja arusaadav „Infoturbe soovituste juhend", mis annab lühiülevaate olulisematest IT-turbe alastest turvameetmetest [25].

2 TOIMEPIDEVUSE TAGAMINE

Toimepidevuse tagamine on protsesside järjepideva toimimise suutlikkus ja taastamise võime pärast katkestust [1]. Tegemist on kestva tugiprotsessiga, mis toetab kõiki ettevõtte põhiprotsesse.

Järgmistes alampeatükkides tutvustatakse toimepidevuse tagamise põhimõtteid ja tegevusi. Tegevuste paremaks mõistmiseks on ära toodud näiteid erinevatest juhenditest ja reaalelulistest praktikatest.

2.1 TOIMEPIDEVUSE TAGAMISE PÕHIMÕTTED

Toimepidevuse peamisteks märksõnadeks on ennetus ja reageerimine. Tähtis on maandada riskid ja koostada toimepidevusplaan. Oluline on mõista, et talitluspidevuse tagamine keskendub äriprotsesside toimimisele, mille komponentideks on peale andmete ka näiteks hooned, infrastruktuur, seadmed ja tarkvara, personal jne.

Toimepidevuse tagamise esimeseks eesmärgiks on kindlustada end maksimaalselt ohtude vastu. Paraku ei ole ka kõige edukama riskijuhtimise juures protsessid kunagi sajaprotsendiliselt kaitstud. Igal ajahetkel võib tekkida katkestus või kriis - negatiivne kõrvalekalle teenuse eesmärgi- ning plaanipärasel osutamisel, mis on põhjustatud kas prognoositavast (näiteks streik) või ootamatust (näiteks elektrikatkestus, torm) sündmusest [28]. Seetõttu on järgmiseks oluliseks eesmärgiks kriisi korral võimalikult kiiresti tööd jätkata.

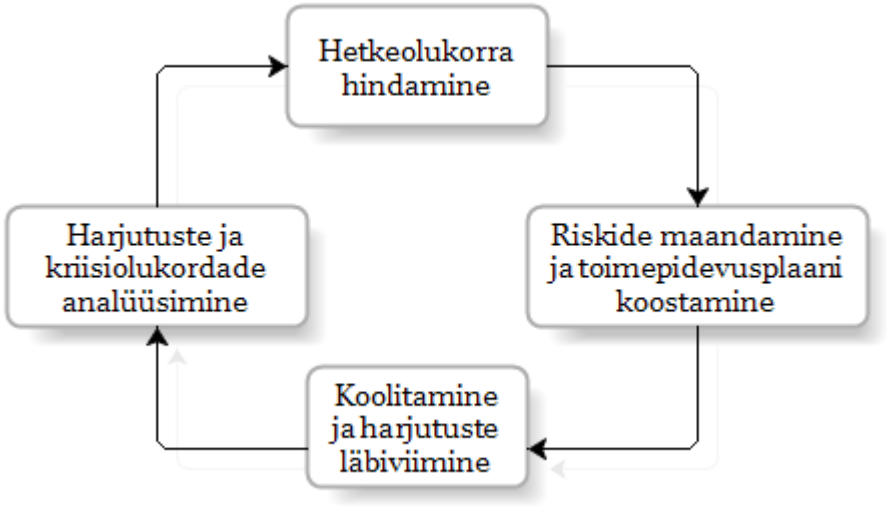
Paljudel ettevõtete ja asutuste juhtidel on valearusaam, et toimepidevuse tagamisega ei ole vaja tegeleda, kui on vormistatud kahjukindlustus. Kindlustus võib küll tasuda otsesed kahjud, kuid ei pruugi katta katkestuse ajal saamata jäänud kasumit. Samuti ei suuda kindlustus taastada ettevõtte mainet ega tagasi võita kliente, kes on kriisi ajal funktsioneerimise lõpetanud teenusepakkuja juurest konkurendi juurde läinud. Elutähtsate teenuste osutajate puhul võivad tagajärjed olla veelgi rängemad – kui teenus ei toimi pika aja vältel, võib see ohustada inimeste elu ja tervist.

Toimepidevuse tagamine koosneb neljast põhilisest faasist:

1. Hetkeolukorra hindamine
2. Riskide maandamine ja toimepidevusplaani koostamine
3. Koolitamine ja harjutuste läbiviimine
4. Harjutuste ja kriisiolukordade analüüsimine

Toimepidevuse tagamine ei ole ühekordne projekt, vaid kestev protsess, mis on oluline osa ettevõtte või asutuse jätkusuutlikust juhtimisest.

Toimepidevuse tagamise tsükkel on illustreeritud joonisel 1.



Joonis 1. Toimepidevuse tagamise tsükkel.

2.2 RESSURSSIDE KAARDISTAMINE

Ressursside kaardistamine annab ülevaate kõikide varade ja vahendite kohta. Enamasti grupeeritakse ressursid loogilistesse kategooriatesse – hooned, infrastruktuur, personal, seadmed, tarkvara, andmed, finantsvahendid, lepingud koostööpartneritega.

Ülevaade olemasolevatest ressurssidest on sisendiks kriisiolukorras alternatiivsete töö jätkamise võimaluste kirjeldamisel. Vaatleme näitena hoonete ressurssi alternatiivide kaalumist.

Alternatiivsete asukohtade määramisel on mitu erinevat valikut:

1. Kui ettevõttel on mitu kontorit, saab kaaluda kriisi ajal teise kontorisse kolimist.
2. Jätkata tööd infrastruktuurita tagavarahoones, kuhu rajatakse kommunikatsioonid ning paigaldatakse seadmed ja tarkvara (aeglasem).
3. Jätkata tööd infrastruktuuriga tagavarahoones, kus on saavutatud valmisolek tööd koheselt jätkama (kiirem).
4. Sõlmida leping vastava teenusepakkujaga, kes pakub kriisi ajal vajalikul määral varustatud kontoripinda.
5. Mõni muu sobilik variant sõltuvalt vahenditest ja võimalustest.

[26]

Alternatiivasukoha valikul võib osutuda oluliseks selle kaugus primaarsest asukohast. Võib esineda olukordi, kus mõlemas asukohas on töö jätkamine võimatu – näiteks laialdaste üleujutuste korral või juhul kui mõlemad sõltuvad ühest ja samast elektrialajaamast, mis ettenägematutel põhjustel rivist välja langeb. Ajalooliselt saab välja tuua 11. septembri terrorirünnakute näite, kus paljudel kaksiktornide läheduses asuvatel ettevõtetel oli küll vähemalt kaks andmekeskust, kuid mõlemad asusid kriisipiirkonnas ja seetõttu oli vaatamata alternatiivasukohtade olemasolule tegevuse jätkamine võimatu [3].

Analoogiline analüüs peab toimuma kõikide oluliste ressursside puhul.

2.3 ÄRIMÕJU ANALÜÜSI KOOSTAMINE

Toimepidevuse tagamise vajaduste ja skoobi mõistmiseks tuleb esimese sammuna koostada ärimõju analüüs (ingl k. *business impact analysis*).

Ärimõju analüüsi koostamisel tuleb läbi viia kolm suuremat loogilist tegevust:

1. Äriprotsesside kaardistamine ja ärimõju hindamine
2. Taastamiseks vajalike ressursside identifitseerimine
3. Äriprotsesside prioriteetide hindamine

[22]

Esimese tegevuse ajal kaardistatakse kõik äriprotsessid ja nende seotus erinevate ressurssidega. Iga protsessi kohta hinnatakse, milline on katkestuse mõju, maksimaalne aeg, mille vältel protsessi toimimine võib olla häiritud mitteaktsepteeritavaid tagajärgi kaasa toomata ning määratakse nõutav taasteaeg [22].

Teise tegevuse ajal luuakse nimekirjad kõikidest füüsilistest ja loogilistest ressurssidest, sh hooned, personal, seadmed, tarkvara, andmed jt varad, mis on vajalikud, et katkestuse järel äriprotsesside toimimist taastada [22].

Kolmanda tegevuse ajal hinnatakse, milliste äriprotsesside toimimine on kõige prioriteetsem ja millised ressursid tuleb esmajärjekorras taastada, et toetada põhitegevuste toimimist [22].

Tabelis 2 esitatakse lihtsustatud näide ärimõju analüüsi koostamisest.

Tabel 2. Näide bussigraafikute koostamise kaardistamisest.

Prioriteet	**Protsess**	**Toimimiseks vajalikud ressursid**	**Nõutav taasteaeg**	**Maksimaalne lubatud maasoleku aeg**
Kõrge	Linnaliini bussi-graafikute koostamine	1. Toimiv infrastruktuur 2. Füüsiline server 3. Graafikute koostamise infosüsteemi tarkvara 4. Andmed liinide, busside, tankimise, bussijuhtide, sõidugraafikute jms kohta 5. Arvuti infosüsteemiga töötamiseks 6. Printer bussijuhtidele graafikute välja printimiseks 7. Inimressurss: vähemalt üks liikluskorralduse spetsialist	2 tundi	1 ööpäev
Katkestuse mõju				
Kui bussigraafikute koostamise infosüsteem läheb maha, siis on võimalik graafikuid koostada ainult liikluskorralduse spetsialistide mälu põhjal. Bussijuhid võivad saada lünklikud ja ebatäpsed graafikud ning linnaliini transport võib kohati katkeda, mis omakorda mõjutab kõiki ühistransporditeenuseid kasutavaid isikuid. Kuna lepingupartner tasub läbitud liinikilomeetrite eest, võib katkestus tekitada suure rahalise kahju. Samuti võib intsidendi meediakajastus oluliselt kahjustada ettevõtte mainet.				

2.4 RISKIANALÜÜSI KOOSTAMINE

Ärimõju analüüsiga on tihedalt seotud riskianalüüs. Esimene defineerib erinevate katkestuste mõju ettevõttele, teine määratleb riskid, mis võivad antud katkestusi põhjustada.

Riskianalüüsiga on seotud kolm põhimõistet:

1. Oht – süsteemi või organisatsiooni kahjustada võiva soovimatu intsidendi potentsiaalne põhjus [27].
2. Nõrkus – vara või vararühma nõrk koht, mida saab ära kasutada oht [27].
3. Risk – võimalus, et vaadeldav oht kasutab ära mingi vara või vararühma nõrkused, põhjustades varade kaotuse või kahjustuse [27].

Riskianalüüsis kirjeldatakse kõik asjakohased riskid ning hinnatakse nende realiseerumise tõenäosust ja tagajärgede mõju. Ettevõte peab vastavalt oma vajadusele valima tõenäosus- ja tagajärgede mõju astmete arvu. Tabel 3 illustreerib, kuidas tõenäosusastmeid teatud kriteeriumite alusel neljaks jagada.

Tabel 3. Näide tõenäosusastmete kohta [21].

Ebatõenäoline	**Võimalik**	**Tõenäoline**	**Väga tõenäoline**
Iga 10 aasta tagant või harvem	Umbes kord aastas	Umbes kord kuus	Kord nädalas või sagedamini

Analoogselt on võimalik jagada tagajärgede mõju „madal”, „normaalne”, „kõrge”, „väga kõrge”. Nende väärtuste põhjal koostatakse 4x4 riskihindamismaatriks, mis on ära toodud tabelis 4.

Tabeli 4. Näide riskihindamismaatriksi kohta [21].

	Mõju				
Tõenäosus		**Madal**	**Normaalne**	**Kõrge**	**Väga kõrge**
	Väga tõenäoline	madal	keskmine	kõrge	väga kõrge
	Tõenäoline	madal	keskmine	kõrge	kõrge
	Võimalik	madal	madal	keskmine	keskmine
	Ebatõenäoline	madal	madal	madal	madal

Lõpptulemusena tekib tabel, kus on kirjeldatud kõik riskid, hinnang nende raskusastmele ja võimalikud leevendusmeetmed. Elutähtsate teenuste osutajad saavad juhinduda ametlikust toimepidevuse riskianalüüsi koostamise juhendist. Lisaks sellele leidub palju inglise ja eesti keelset kirjandust erinevate kvantitatiivsete ja kvalitatiivsete riskihindamise metoodikate kohta.

Riske saab klassifitseerida ja grupeerida erinevalt. Toimepidevuse riskianalüüsi koostamise juhend pakub välja neli erinevat riskikategooriat:

1. Inimtegevus
2. Loodussündmused
3. Tehnoloogilised ohud
4. Majanduslikud ja õiguslikud ohud

[28]

ISKE etalonturbe süsteem on ohud koondanud kuute moodulisse:

1. Vääramatud jõud
2. Organisatsioonilised puudused
3. Inimvead
4. Tehnilised rikked ja defektid
5. Ründed
6. Andmekaitseohud

[29]

Riske võib vastavalt vajadusele klassifitseerida ka detailsemateks gruppideks, oluline on riskide süstemaatiline analüüs ja võimalikult suur ohtude spektri katmine.

Riske hinnates tuleb lähtuda ettevõtte või asutuse individuaalsetest karakteristikutest. Näiteks geograafilisest aspektist saab Eestis maavärinate, hiidlainete ja vulkaanipursete tõenäosuse madalaks hinnata. Samas tuleb teatud regioonides arvestada üleujutuste ja metsapõlengutega. Üks rängimate tagajärgedega kriis oli 2005. aasta üleujutus Pärnus, mis halvas päevadeks mitmete ettevõtete töö ja tõi endaga kaasa Eesti lähimineviku suurima kindlustuskahju [30]. Positiivse näitena võib tuua rannarajooni hotelli Viiking, mille meeskond valmistus üleujutusteks tõstes arvutid maapinnast kõrgemale. Tänu sellisele lihtsale meetmele õnnestus seadmed ja dokumendid päästa [31]. Siinkohal tuleb arvestada, et veekahjustusi võib tekitada ka vigastatud sprinkler või purunenud veetoru ning ühel ohul võib olla erinevaid allikaid.

Riske määratledes tuleb tähelepanu pöörata ka koostööpartnerite osale. Näiteks kui andmete majutamise osas on sõlmitud leping mõne välise teenusepakkujaga, tuleb arvestada et laialdasema kriisi korral võib tekkida olukord, kus on vaja taastada mitme erineva ettevõtte või asutuse andmed korraga. Sellisel juhul peavad lepinguga olema määratletud prioriteedid ja kriteeriumid, mille alusel teenusepakkuja taastamisjärjekorra moodustab.

2.5 RISKIDE MAANDAMINE

Eelmises faasis koostatud riskianalüüs identifitseerib ohud ja nõrkused. Järgmine samm riskihalduses on otsustada, milliseid tegevusi sooritada riskide maandamiseks.

Antud tegevuseks on neli erinevat lähenemist:

1. Vältimine – hoidutakse tegevustest, mis endaga antud riski kaasa toob.
2. Leevendamine – püütakse vähendada riski realiseerumise tõenäosust või sellega kaasnevaid tagajärgi.
3. Jagamine – riski üle kandmine teisele osapoolele, tüüpiliselt mõeldakse selle all kindlustamist.

4. Aktsepteerimine – ollakse valmis vastu võtma kahjumit riski realiseerumisel. Enamasti kasutatakse antud lähenemist juhul, kui riski maandamise kulud ületavad potentsiaalse kahju ajalises lõikes.

[32]

Riskide maandamisel on oluliseks mõisteks turvameetmed – riski kahandavad teguviisid, protseduurid või mehhanismid [27].

Turvameetmed jagunevad otstarbe järgi ennetavateks, avastus- ja taastusmeetmeteks. Teostusviisi järgi saab neid liigitada organisatsiooniliseks, füüsiliseks ja infotehnoloogilisteks [27]. Tabelis 5 on esitatud mõningaid näiteid võimalikest meetmetest, mida rakendada teatud riskide maandamiseks.

Tabel 5. Näiteid erinevatest riskidest ja nende maandamisest.

Risk	**Võimalikud rakendatavad meetmed**
Võtmetöötaja surm	1. Määrata ajutine asetäitja, kes on valmis kohe kohustusi üle võtma. 2. Kui tegemist on ainsa inimesega, kellel on ligipääs teatud süsteemidele, siis dubleerida paroolid seifi kinnisesse ümbrikusse või leida teine viis säilitada ligipääs.
Andmete hävimine	1. Teha regulaarselt varukoopiaid. 2. Testida varukoopiate tegemise ja neist taastamise protsessi. 3. Hoiustada varukoopiad erinevates asukohtades piisavalt kaugel originaalandmetest, et vältida nende üheaegset hävinemist. 4. Koolitada töötajaid andmetega õigesti ümber käima ja rakendada ligipääsuõiguste süsteemi. 5. Harida töötajaid viiruste, häkkerite ja sabotaaživõimaluste osas.

Riskijuhtimine on üheks eelduseks edukale talitluspidevuse tagamisele.

2.6 TOIMEPIDEVUSPLAANI KOOSTAMINE

Isegi eduka riskijuhtimise korral ei ole ettevõtte äriprotsesside toimimine kunagi sajaprotsendiliselt tagatud. Kui intsident juhtub, peavad vastutavad isikud olema valmis seda võimalikult kiiresti lahendama – selleks peab juba varasemalt olema koostatud efektiivne toimepidevusplaan, mille järgi toimida.

Esimene samm on kindlaks määrata, kelle ülesanne on toimepidevuse juhtimine ja plaani koostamine. Siin on võimalik võtta kaks erinevat suunda – ettevõte hoolitseb ise toimepidevuse tagamise eest ning selleks on piisavalt ressurssi ja kompetentsi või ettevõte ostab vastavat teenust.

Juhul kui ettevõte otsustab toimepidevusplaani ise koostada, peavad meeskonnas olema täidetud vähemalt kolm rolli:

1. Isik, kellel on toimepidevuse alaseid kogemusi.
2. Isik, kellel ülesandeks jääb toimepidevusplaani hooldamine ja uuendamine pikema aja vältel.
3. Isik, kellel on väga head teadmised ettevõtte süsteemide ja protsesside kohta.

[26]

Kui ettevõttel vastav kompetents puudub, saab toimepidevuse tagamise teenust sisse osta ning sellisel juhul täidab esimest rolli teenusepakkuja. Hetkel pakuvad Eestis talitluspidevuse juhtimise teenust näiteks Hansson, Leego & Partner, Consult IT, KPMG ja teised IT-konsultatsiooni firmad [33, 34, 35].

Toimepidevusplaanid võivad erineva suurusega ettevõtetel olla väga erinevad nii sisu, mahu kui ka detailsuse osas. Sellegipoolest on talitluspidevusplaanis teatud kindlad komponendid, mis peavad olema esindatud.

Plaan peab koosnema vähemalt järgmistest osadest:

1. Plaani eesmärk – esitab selgelt plaani otstarbe ja oodatava tulemuse.
2. Plaani kasutuselevõtu ja hädaolukorra lõpetamise tingimused – defineerib tingimused, mille alusel kuulutatakse välja või lõpetatakse kriisiolukord ja kellel on volitused seda teha.

3. Töötajate andmed – talitluspidevuse tagamisega seotud kriisimeeskondade töötajate ajakohastatud andmed.
4. Kriitiliste tegevuste minimaalse toimepidevuse nõuded – ärimõju analüüsi raames välja selgitatud prioriteetsete protsesside katkestuse maksimaalne lubatud kestus.
5. Ressursside loetelu ja asukoht – ärimõju analüüsi raames välja selgitatud prioriteetsete protsesside taastamiseks vajalikud ressursid ja info nende asukoha kohta.
6. Teenuse osutamise alternatiivasukoht – asukoht, kuhu protsessid liigutatakse kriisi ajal, vajalike ressursside transpordi korraldus ja ajutise kriisikeskuse info.
7. Detailsed taastestsenaariumid – protseduurid katkestuse likvideerimiseks ja konkreetse taastamisoperatsiooni eest vastutaja(d). Enamasti luuakse iga süsteemi jaoks individuaalsed taasteplaanid.
8. Töötajate ohutuse tagamine – protseduurid töötajate ohutuse tagamiseks, sh evakueerimine jt asjakohased meetmed.
9. Katkestusest teavitamise korraldus – korraldus, mis määrab kindlaks kriisikommunikatsiooni reeglid, so kuidas ja millal teavitatakse töötajaid, kliente ja koostööpartnereid ning avalikkust. Määratleb, kes on vastutav infovahetuse korraldamise eest. Sisaldab ka juhiseid, kuidas käituda, kui sidevahendite kasutamine on häiritud.
10. Plaani testimine – määrab, kui tihti plaani testitakse, millises ulatuse ning millised on oodatavad ja saavutatud tulemused.

[22, 23, 26, 36]

Toimepidevusplaan peab olema juhtkonna poolt kinnitatud.

Valminud toimepidevusplaani juures on väga oluline, et see on õigel hetkel kättesaadav. Mõistlik on plaani hoida erinevates asukohtades, nii digitaalsel kui ka paberkujul ja piisava arvu koopiatega.

2.7 KOOLITAMINE

Koolitusprotsess on oluline osa toimepidevuse tagamisel. Ka väga hea plaan ei pruugi toimida, kui taastamisega tegelevad inimesed ei ole seda kordagi enne kriisi realiseerumist

näinud. Seega on oluline osa kriisiks valmistumisel toimepidevusplaani olemasolu teadvustamine ja selle tutvustamine.

Koolitusi on vajalik korraldada vähemalt korra aastas [22, 37]. Selle eesmärk on tagada, et iga töötaja teab, keda kriisi korral teavitada ja millised on tema ülesanded. Koolituste käigus tuleb laiali jagada ka toimepidevusega seotud juhendmaterjalid, mis võimaldavad töötajatel nendega tutvuda ka hiljem.

Koolitusi saab eristada vastavalt sihtgrupile:

1. Tavatöötajatele suunatud koolitused keskenduvad põhitegevuste teadvustamisele – milline on kriisi ajal käitumise kord ja kuidas teavitada juhendavaid isikuid.
2. Konkreetse kriisimeeskonna koolituste eesmärk on vaadelda süvendatult erinevate ohuolukordade lahendamist.
3. Tippjuhtkonnale suunatud koolitused on strateegilise fookusega.

[37]

2.8 HARJUTUSTE LÄBIVIIMINE

Põhiliselt kasutatakse harjutuste läbiviimiseks kahte erinevat lähenemist:

1. Perioodiline testimine
2. Ohuolukordade simuleerimine

Perioodilise testimise korral katsetatakse infosüsteemide taastamist teatud intervallide tagant, vähemalt kaks korda aastas. Sellise testimise raames liigutatakse kõik kriitilised süsteemid alternatiivsesse asukohta ja testitakse, kas protsessid käivituvad seal tõrgeteta. [24, 26].

Perioodiline testimine on väga kulukas, kuna sellised harjutused toimuvad töötundide ajal ning nõuavad paljude talitluspidevuse tagamisega seotud töötajate osalust [26].

Kuna perioodiline testimine on kulukas, täiendatakse seda taasteharjutuste simuleerimise abil. Talitluspidevuse tagamise võtmeisikud kogutakse meeskondadesse erinevate laudade ümber – primaarse asukoha meeskond, alternatiivse asukoha meeskond jne. Neile antakse

paberil võimaliku katkestuse stsenaarium ja osalejad mängivad etteantud olukorra läbi. Kõik meeskonnaliikmed täidavad stsenaariumi põhjal spetsiaalsed ankeedid, kuhu nad peavad märkima, keda nad teavitavad ja milliseid samme ette võtavad, et süsteemide tööd võimalikult kiiresti taastada [26].

Simuleerimise eeliseks on võimalus kiirelt läbi mängida erinevate stsenaariumite erinevaid etappe, nt üks etapp algab hommikul kell 9 ning järgnev kirjeldab olukorda 12 tundi hiljem [26].

Iga testi kohta peab tekkima testimisprotokoll, mis sisaldab järgmisi elemente: testi eesmärk ja ulatus, toimumise aeg, testi kaasatud ressursid, testi läbiviija, testi tulemused [24].

Kui test on lõppenud, hinnatakse selle edukust. Testimise protokolli analüüsi alusel viiakse läbi muudatused talitluspidevusplaanis, seda tagavas meeskonnas ja tagavararessursside osas [24, 26].

Toimepidevusplaani muudatuste kohta peab tekkima logi, mis kirjeldab muudatusi ja nende läbiviimise aega. Samuti tuleb korraldada muudatustest teavitamine.

2.9 KRIISIMEESKONNA KOOSTAMINE

Põhiküsimuseks toimepidevuse tagamise juures on intsidendijärgse töö taastamine. See peab toimuma sujuvalt ja võimalikult kiiresti ning selleks on vaja efektiivset meeskonda, kus üksikisikute ja gruppide ülesanded on võimalikult selged ja määratletud. Enamikes suuremates arenenud talitluspidevuse juhtimisega ettevõttes on kriisimeeskonna struktuur kolmetasemeline:

1. Esimene tase – Kriisipoliitika töörühm
2. Teine tase – Kriisireguleerimismeeskond
3. Kolmas tase – Operatiivrühmad

[26]

Kriisipoliitika töörühm koosneb juhtidest, kes võtavad vastu otsuseid ja määravad erakorraliste finantsvahendite kasutamist kriisi ajal. Samuti on nende ülesanne kinnitada

kriisireguleerimismeeskonna otsuseid ja hinnata läbiviidavate tegevuste mõju pikemas perspektiivis. Kriisipoliitika töörühma kuuluvad enamasti juriidilise üksuse, personali-, avalike suhete juhid ja finantseksperdid [26].

Kriisireguleerimismeeskond allub kriisipoliitika töörühmale ja koosneb ettevõtte osakonnajuhtidest ja teistest võtmeisikutest. Nende peamised ülesanded on tagada personali ohutus, kriisiaegsete tegevuste koordineerimine ja hilisem taastamine. Kriisireguleerimismeeskonna juht peab olema isik, kes tunneb väga hästi ettevõtte struktuuri, süsteeme ja protsesse [26].

Operatiivrühmad on väiksemad üksused, mis alluvad kriisireguleerimismeeskonnale. Iga meeskond saab endale ülesandeks tegeleda ühe kitsama valdkonnaga, näiteks logistika, kindlustuse või telekommunikatsioonidega [26].

Meeskonna koostamisel on kõige olulisem kindlaks määrata üks kriisijuht, kellele alluvad kõik väiksemate üksuste juhid. Tähtis on paika panna kõikide võtmeisikute volitused ja vastutusalad. See väldib olukordi, kus juht ei saa tegutseda ebapiisavate volituste tõttu, jääb ebaselgeks, kes vastutab millise osa eest, või tekib olukord, kus erinevad osakonnad ei suuda koostööd teha.

Kui kriisi lahendamiseks on vaja meeskonda kaasata välised koostööpartnerid, peab olema selgelt määratletud, kuidas ja millal toimub nende teavitamine ning millised on nende volitused ja ülesanded.

2.10 KRIISIKOMMUNIKATSIOON

Kriisikommunikatsioonil on väga oluline roll kriiside kiirel ja efektiivsel lahendamisel.

Saab eristada kahte liiki kommunikatsiooni:

1. Sisekommunikatsioon – suhtlus ettevõttesiseselt erinevate osakondade ja töötajate vahel.
2. Väliskommunikatsioon – suhtlus klientide, välispartnerite ja meediaga.

Sisekommunikatsioon põhieesmärgiks on tagada informatsiooni jõudmine vajalike osapoolteni, et langetada adekvaatseid otsuseid ja kriis võimalikult efektiivselt lahendada.

Segaduste vältimiseks peab talitluspidevusplaanis olema kirjas, milliseid sidevahendeid (ja nende alternatiive) kriisi ajal kasutada ja keda tuleb teavitada. Samuti peavad olema saadaval kõikide seotud töötajate kontaktandmed – nimed, rollid, telefoninumbrid (ametlikud ja isiklikud) [26].

Sisekommunikatsiooni head tavad ja põhimõtted:

1. Kriisi või kriisiohu avastaja ei tohi asja jätta ainult enda teada.
2. Kommunikatsioon ei tohi olla emotsionaalne, tuleb edastada ainult kindlaid fakte, mitte eeldusi või oletusi.
3. Kriisijuhi ülesanne on otsuste tegemine ja tegutsemine, teavitamine tuleb anda kellegi teise ülesandeks.
4. Tuleb luua kriisikeskus, kus kriisireguleerimismeeskond saab näost-näkku suhelda ja ühiselt edasisi strateegiaid arutada.
5. Ettevõttesiseselt infot ei filtreerita – otsustajad ja kõneisik peavad olema kõikide asjaoludega kursis.
6. Andes korralduse tuleb küsida, kuidas saaja sellest aru sai.
7. Kommunikatsiooni eesmärgiks peab olema intsidendi võimalikult kiire lahendamine mitte süüdlase otsimine.

[36, 38]

Kui sisekommunikatsiooni eesmärgiks on võimalikult kiiresti võimalikult palju asjakohast infot edasi anda, siis väliskommunikatsiooni eesmärgiks on piisavas koguses adekvaatse info edastamine. Põhiküsimuseks on siin ettevõtte maine kaitsmine ning klientide, koostööpartnerite ja avalikkuse teavitamine.

Enne teavitamist või avalduste tegemist tuleb analüüsida kriisi mõju klientidele, koostööpartneritele, organisatsioonile, ühiskonnale ja teistele seotud osapooltele [38].

Elutähtsate teenuste osutajatel on hädaolukorra seadusest tulenev kohustus avalikkust teavitada kriisiolukorras [1].

Avalikkuse teavitamiseks on erinevaid vahendeid – ettevõtte koduleht, blogi, sotsiaalmeedia (Facebook, Twitter), suhtlus meediaga. Talitluspidevusplaanis peab olema selgelt määratletud, milliseid suhtluskanaleid kasutatakse, kes on ettevõtte kõneisik ja kes kuuluvad teavitusgruppi.

Meediasuhtluse põhimõtted:

1. Ettevõttel on vaid üks kõneisik ja töötajad ei esine meedias.
2. Tuleb üle kontrollida, kas faktid vastavad tõele, ei tohi spekuleerida ega eeldada.
3. Kui infot ei ole, siis tuleb nii öelda, kuid vältimaks meedia spekulatsioone tuleb info välja uurida ja edastada esimesel võimalusel.
4. Tuleb kontrollida meediasituatsiooni (kus, millal ja kuidas infot edastatakse) ja salvestada meediakontaktid (kellele, millal ja mida öeldi).
5. Kui meediasse teatati vigane info, siis tuleb viga kohe parandada, et vältida usaldamatuse teket.
6. Kriisiolukorras ei tohi iialgi öelda ainult „ei kommenteeri", sest see näitab, et informatsiooni varjatakse tahtlikult. Kui ei saa kommenteerida, siis tuleb seda põhjendada.
7. Tuleb vältida korraga mitme erineva info andmist ja rõhutada algset sõnumit.
8. Meediaga suhtleja peab olema aus ja abivalmis.
9. Meediaga suheldes peab jääma rahulikuks ja konkreetseks.
10. Meediat ei tohi ignoreerida, samuti tuleb ise alustada suhtlemist meediaga, et vältida olukorda, kus meedia avaldab kontrollimata esmase vaatluse infot.

[36, 38, 39]

2.11 INVESTEERINGUTE PLANEERIMINE

Toimepidevuse üks põhiküsimusi on „Kui palju investeerida talitluspidevuse tagamisse?". Eelarve koostamise protsess on keeruline, kuna riskide realiseerumise tõenäosust arvestades ei ole võimalik ette ennustada, kas risk realiseerub kümne aasta pärast, mitte kunagi või homme.

Tänapäeval on üks levinumaid valearusaamu, et toimepidevuse tagamise kulud ületavad katkestusest tuleneva kahju, kuna tihtipeale ei suudeta kahju reaalset ulatust adekvaatselt hinnata. Samuti tekib tihti olukordi, kus vastutavad isikud arvavad, et katkestuse tekkimine on äärmiselt ebatõenäoline ning peavad talitluspidevuse tagamist tarbetuks lisakohustuseks

[26]. Seetõttu on oluline leida sobiv lähenemine, mis kindlustab tasakaalu efektiivse riskide maandamise ja selleks kulunud ressursside vahel.

Järgnevalt tutvustatakse nelja lähenemist talitluspidevuse tagamise eelarve koostamiseks.

1. Tõenäosusel baseeruv lähenemine (ingl k *probability-based approach*)
2. Järelevalve reeglite meetod (ingl k *prudent person methodology*)
3. Intuitiivne otsustusmeetod (ingl k *intuition-based executive approach*)
4. Ettenägeliku usaldusanalüüsi lähenemine (ingl k *prudent fiduciary analysis approach*)

Tõenäosusel baseeruva lähenemise korral korrutatakse katkestuse esinemise tõenäosus ja katkestusest tulenev potentsiaalne kahju ja võrreldakse seda alternatiivsete töö jätkamise meetodite rakendamise maksumusega. Sellise lähenemise korral võib tekkida situatsioon, kus väga madala tõenäosusega kriisi realiseerumise korral on kahjud nii suured, et ettevõte läheb pankrotti [26]. Seetõttu ei peeta tänapäevaste missioonikriitiliste protsesside juures tõenäosusel baseeruvat lähenemist parimaks.

Järelevalve reeglite meetodi korral elimineerivad juhtisikud kõik alternatiivsed talitluspidevuse tagamise võimalused, mis ei ole kvaliteedilt aktsepteeritavad ettevõtte või asutuse lühi- ja pikaajalise arengu seisukohast. Seejärel valivad analüütikud ülejäänud variantide hulgast kõige madalama kuluga alternatiivi, mis võimaldab süsteeme taastada ettenähtud aja jooksul [26].

Intuitiivne otsustusmeetod on välja kujunenud Richard Cyerti ja James Marchi 1963. aastal välja pakutud konflikti lahendamise metodoloogiast, mis on tänapäeval aluseks mitmetele ekspertsüsteemidele. Selle teooria järgi tuleb identifitseerida põhilised hinnangukriteeriumid ja nendega seotud võtmeisikud [40]. Näiteks juhtide eesmärgiks on tagada ettevõtte või asutuse jätkusuutlikkus, infosüsteemide haldajatel taastada võimalikult kiiresti ja väheste kahjudega antud süsteemide toimimine ning finantsanalüütikutele on oluline kulude minimiseerimine pikas perspektiivis. Kõik erinevad tagavararessursid saavad mõõdikud, nt kasumi ja kahjumi suhe, maasoleku aeg, antud alternatiivi maksumus. Seejärel otsustavad võtmeisikud, millised alternatiivid on aktsepteeritavad nende seisukohast. Valituks saab osutuda ainult variant, mis on kõigi osapoolte poolt aktsepteeritav. Kui selliseid variante on mitu, valitakse enamasti odavaim lahendus [26].

Ettenägeliku usaldusanalüüsi lähenemise korral kasutatakse Cyerti ja Marchi metodoloogiat, kuid võetakse arvesse ka klassikalisi mikroökonoomika ja ettevaatlikkuse printsiipe. Selle aluseks on eeldus, et juhid on intuitiivsed ja spetsialistid analüütilised. Antud lähenemise korral elimineerivad juhid variandid, mis ei ole aktsepteeritavad ettevõtte või asutuse jätkusuutlikkuse osas ning spetsialistid võrdlevad ülejäänud valikuid kasumi maksimiseerimise ja riskide minimiseerimise aspektist [26].

3 TOIMEPIDEVUSE TAGAMISE KORRALDUS AVALIKE TEENUSTE OSUTAMISEL EESTIS

Avalik teenus on avalike ülesannete täitmisel üldistes huvides osutatav teenus, mis on suunatud avalike hüvede pakkumisele, avaliku ülesandega kaasneva kohustuse täitmisele või põhiõiguste, vabaduste ja huvide kaitsele [41].

Suur osa Eesti avalikest teenustest on kättesaadavad e-teenustena. Ka paljud ülejäänud teenused põhinevad spetsiifilistel infosüsteemidel või jätavad kohustusliku jälje maha asutuste ja ettevõtete dokumendihaldussüsteemidesse. Süsteemid muutuvad aina keerulisemaks ning seetõttu suureneb ka vajadus IT-alase toimepidevuse aspektid laiemalt läbi mõelda.

Avalike teenuste toimepidevuse aspektist on võimalik eristada kahte suurt gruppi teenuseid – ISKE-ga reguleeritud andmekogudel põhinevad teenused ja hädaolukorra seadust täitvad elutähtsad teenused.

Järgmistes alampeatükkides esitatakse ülevaated mõlema teenusegrupi toimepidevuse tagamise olukorrast.

3.1 ANALÜÜSI LÄBIVIIMISE METOODIKA

Toimepidevuse tagamine on delikaatne teema, mis on otseselt seotud asutuse infoturbe ja julgeolekuga. Elutähtsate teenuste osutajate nimekiri ei ole avalikult kättesaadav, samuti ei ole selgelt ja üheselt määratletud, millistele avalike teenuste osutamiseks vajalikele andmekogudele peab ISKE-t rakendama. Sellises olukorras on välistatud võimalikult suure valimi pealt küsitluse või muus analoogses vormis statistilise analüüsi läbiviimine.

Valdkonnast ülevaate saamiseks ja eesti avalike teenuste olukorra hindamiseks viidi antud magistritöö autori poolt läbi seitse intervjuud (tabel 6).

Tabel 6. Läbiviidud intervjuud.

Funktsioon	**Asutus**	**Intervjueeritav (amet)**
Elutähtsate teenuste koordineerija riiklikul tasandil	Riigi Infosüsteemi Amet	Epp Maaten (riskijuht, nüüdsest Järelevalve osakonna juhataja kt)
Elutähtsa teenuse osutaja statsionaarse eriarstiabi valdkonnas	TÜ Kliinikum	Eiko Pruks (Informaatikateenistuse direktor)
ISKE koordineerija riiklikul tasandil	Riigi Infosüsteemi Amet	Aare Reintam (ISKE valdkonnajuht)
ISKE rakendaja	Tartu Linnavalitsus	Jüri Mölder (Linnasekretär)
Elutähtsa teenuse toimepidevust korraldav asutus	Tartu Linnavalitsus	Rein Haak (Linnamajandamise osakonna juhataja)
Toimepidevuse alase seadusandluse ettevalmistaja	Siseministeerium	Hannes Unt (Pääste- ja kriisireguleerimispoliitika osakonna nõunik kt)
Elutähtsa teenuse osutaja omavalitsuse ühistranspordi valdkonnas	AS SEBE	Tõnu Ruusamäe (piirkondlik juht Tartus)

Intervjueeritavad on valitud lähtuvalt järgmistest põhimõtetest:

1. Olukorra hindamiseks valiti asutused eesmärgiga saada ülevaadet teenuste osutamise protsessist eri tasanditel – alates teenuseosutajatest ja neid reguleerivatest üksustest kuni vastava seadusandluse elluviijateni.

2. Elutähtsate teenuste osutajate seast valiti asutused, mis on vastandlikud oma parameetritelt: väike teenuseosutaja vs suur teenuseosutaja, pika toimepidevuse tagamise kultuuriga vs lühikese praktiseerimisajaga, ministeeriumi haldusalas vs kohaliku omavalitsuse haldusalas.

Kõigi intervjuude kohta on koostatud detailsed memod. Memod ei kuulu avaldamisele antud magistritöös. Kaitsmiskomisjoni liikmetel on võimalus soovi korral konkreetse intervjuu memo näha tingimusel, et selleks on saadud intervjuul osalejate kirjalik nõusolek.

Peatükkides 3.2 ja 3.3 esitatud ülevaated on kooskõlastatud intervjueeritavatega.

3.2 ISKE-GA REGULEERITUD AVALIKUD TEENUSED

3.2.1 KIRJELDUS

ISKE on infosüsteemide kolmeastmeline etalonturbe süsteem, mille väljatöötamisel ja arendamisel on aluseks võetud Saksamaa riikliku infoturbeameti BSI poolt avaldatav infoturbe standard [42].

Andmeturbes vaadeldakse kolme põhikomponenti – andmete terviklikkus, konfidentsiaalsus ja käideldavus.

1. Käideldavus – nõuded töökindlusele ja jõudlusele [25].
2. Terviklikkus – andmed peavad olema täielikud ja muutmata [25].
3. Konfidentsiaalsus – info peab olema kaitstud volitamata avalikustamise eest [25].

Rakendades kolmele komponendile neljapallilist skaalat määratakse turvaosaklassid. Turvaosaklasside kombinatsiooni alusel moodustub andmete turvaklass (nt. K2T3S1). Andmete turvaklassi alusel määratakse andmekogule turbeaste – kõrge (H), keskmine (M) või madal (L) [43]. Turbeaste on aluseks infovarade kaitsemeetmete valimisel ISKE etalonmeetmete kataloogist.

Enamike avalike teenuste aluseks on andmekogud, millele on pandud kohustus rakendada ISKE turbesüsteemi. Kuna avalike teenuste toimepidevuse tagamine on tihti ainult eelmainitud süsteemiga reguleeritud, siis räägitakse edaspidi toimepidevuse tagamisest ISKE rakendamise kontekstis.

3.2.2 SEADUSLIKUD REGULATSIOONID

Hetkel on üheselt määratlemata, mida mõistetakse andmekogu all ning millistele andmekogudele tuleb ISKE-t rakendada. ISKE rakendamise kohustust on defineeritud mitmes erinevas kehtivas seaduses ja määruses.

Avaliku teabe seaduses kasutatakse andmekogudest rääkides termineid „riigiasutus", „kohalik omavalitsus", „kohaliku omavalitsuse asutus" ja „kohaliku omavalitsuse üksus" [11, 44].

Antud seaduse alusel kehtestatud infosüsteemide turvameetmete süsteemi määruses ei ole käsitletud kohalike omavalitsuste asutusi ega üksusi ning selle järgi tuleb ISKE-t rakendada ainult kõikidele riigi ja kohalike omavalitsuste andmekogudele [43].

Infosüsteemide andmevahetuskiht X-tee määrus sätestab ISKE rakendamise kohustust kõigile X-teega liitujatele [45].

3.2.3 ISKE RAKENDAMISE ÜLEVAADE

Infosüsteemide turvameetmete süsteemi määrus jõustus 1. jaanuaril 2008.

Määrusega on sätestatud järgmised tähtajad:

1. Turbeastmega H andmekogu esmakordne auditeerimine – hiljemalt 1. märts 2010
2. Turbeastmega M andmekogu esmakordne auditeerimine – hiljemalt 1. detsember 2010
3. Turbeastmega L andmekogu esmakordne auditeerimine – hiljemalt 1. märts 2011

[43]

Umbes 80% ministeeriumitest on kinnitanud, et nad on ISKE rakendanud, neist 70% on lasknud end auditeerida. Omavalitsustel on ISKE rakendamisel puudujääke. Ka intervjueeritud ISKE rakendaja kinnitas, et protsessiga ollakse teel, kuid ei ole veel lõpuni jõutud.

Hetkel on tugevaimad ISKE rakendajad kaks Eesti riigi suuremat avaliku sektori IT-organisatsiooni – Registrite ja Infosüsteemide Keskus ja Siseministeeriumi

infotehnoloogia- ja arenduskeskus. Eeskujuks saab tuua Registrite ja Infosüsteemide Keskuse, kes on kogu oma haldusala põhiselt ISKE ära rakendanud ja ka ära auditeerinud. Siseministeeriumi infotehnoloogia- ja arenduskeskus on küll ISKE-t rakendanud, kuid ei ole eraldanud raha auditi läbiviimiseks.

ISKE rakendamisel kasutatakse enamasti spetsialiste majas sees. Teenuse sisse ostmise vs ise rakendamise osakaalud on hinnanguliselt 30 vs 70 protsenti. Piisavalt ressurssi omavad asutused tellivad enamasti kõigepealt konsultatsiooni – konsultant saab teha dokumentide kava ja plaanid ja näidata ette, millist joont mööda liikuda, seejärel hakkab edasise rakendamisega tegelema kohalik üksus, näiteks vastava asutuse IT teenistus. Mitmed suuremad asutused on ISKE omal käel rakendanud, näiteks Kultuuriministeerium, Haigekassa, Registrite ja Infosüsteemide Keskus, Siseministeeriumi infotehnoloogia- ja arenduskeskus ning Rahandusministeerium.

Mais 2010 viidi läbi küsitlus 73 ISKE rakendaja seas. Küsitlus annab ülevaate, millises järgus on antud protsess ning millised tegevused on juba selle raames läbi viidud [46].

3.2.4 TOIMEPIDEVUSE TAGAMISE VÄLJAKUTSED

ISKE rakendamise edukus tervikuna sõltub suurel määral ressursside olemasolust. Turvameetmete rakendamise kohustus tuli samal ajal Eestit tabanud majandussurutisega – ajal mil hakati teostama kokkuhoiumeetmeid, mille tulemusena vähendati personali ja investeeringute mahtu. Intervjueeritud ISKE-t rakendava asutuse IT eelarve on viimased viis aastat vähenenud. Sellisel tasemel saab läbi viia ainult hädavajalikud tegevused. Nende tegevuste hulka ei kuulu enamasti analüüsi läbi viimine, protsesside kaardistamine või riskide maandamine.

Teine oluline mõõde on IT-alase toimepidevuse tagamise vajaduse mõistmine. Kõik intervjueeritavad nõustuvad, et IT-sõltuvus kasvab lähiaastatel oluliselt. Infosüsteemide tähtsus on juba praegu igapäevatöös väga suur – kõik asjaajamised on nendega seotud ning kui süsteemid ei toimi, siis tööd teha ei saa. Parimaks näiteks on siin dokumendihaldussüsteemid, mis toetavad kõiki teisi tööprotsesse. Tihtipeale ei tajuta kui suur on sõltuvus infosüsteemidest. Esineb juhtumeid, kus tippjuhtkond näeb toimepidevuse tagamise rahastamise vajadust alles siis, kui toimub suurem katkestus. Ennetustööd on vähe ning ei mõisteta, et intsidentide tagajärgede likvideerimine võib olla oluliselt kallim

kui ennetamine. Ka ISKE rakendamise olemuse mõistmine on keeruline. Palju erinevaid nõudeid ei tähenda palju erinevaid määruseid ja kordasid, kuid paljudes asutustes taandub rakendamine hulgaliselt abstraktsete dokumentide kirjutamisele.

Üheks suurimaks probleemiks ISKE rakendamisel on selle ülesandega tegeleva meeskonna koostamine. Tihti ei ole asutuses kompetentsi ISKE rakendamiseks tervikuna. Kuna ISKE koosneb 60% IT ja 40% füüsilistest ja organisatoorsetest meetmetest, peab määratud meeskond suutma ära katta olemuslikult väga erinevad aspektid. Esineb ka juhtumeid, kus palgatakse spetsiaalne inimene ISKE-t rakendama ning kui auditeerimine on edukalt läbitud, loobutakse tema teenetest. Toimepidevuse tagamist ei vaadelda kui kestvat protsessi.

Toimepidevuse tagamisel ei saa toetuda täies mahus ainult ISKE-le. Kui Saksamaa BSI hakkab välja töötama meetmeid uute tehnoloogiate turvamiseks, siis on need moodulid Eestisse jõudes juba aasta vanad. Kaetud peavad olema ka uued ohud – näiteks tavapäraste arvutite kõrvale on tulnud nutitelefonid ja tahvelarvutid, mida on vaja samuti turvata. Hetkel loob Riigi Infosüsteemi Amet operatiivselt taoliste uute aspektide katmiseks soovituslike turvameetmete juhendeid.

Eelmainitud mais 2010 läbi viidud küsitluses on palutud hinnata ISKE rakendamist takistavaid tegureid. 70% vastajatest põhjendavad, et on liialt palju „tulekahjusid" ja seetõttu ei ole aega ISKE rakendamisega tegeleda ning 37% toob põhjusena välja rahapuuduse. 30% vastajaid on võrdselt põhjustena välja toonud ka ISKE rakendustööriista puudumise ja fakti, et lõppkasutajad ei pea infoturbealaseid tegevusi oluliseks [46].

3.2.5 KATKESTUSED JA NENDE HALDUS

Viimastel aastatel ei ole olnud suuremaid turvaintsidente konfidentsiaalsuse ja terviklikkusega. Kõik suuremad juhtumid on olnud seotud käideldavusega.

Kõige tüüpilisemad katkestuste põhjused on järgmised:

1. Infosüsteemide arhitektuurivead
2. Kolmandatest osapooltest põhjustatud probleemid (eriti liidestatud süsteemides)
3. Mitme halva asja kokkusattumus

Ülejäänud katkestustest enamuse moodustavad riistvara rikked ja elektrikatkestused. Looduslikest ohtudest on Eesti tingimustes kahju teinud äikesetormid – üheks näiteks on juhtum, mil langes rivist välja hinnaline *switch*, mis sai mööda vaskkaableid tabamuse, kuna võrku ei jõutud veel fiiberkaablitega uuendada.

Kõrgkäideldavad süsteemid peaks olema väga tõrkekindlad, kuid tihtipeale on Eestis loodud lahendused nii keerukad, et ISKE meetmed ei kata kogu süsteemi. Seetõttu tuleks arvestada, et ISKE on vaid üks abivahend toimepidevuse tagamisel ja see ei pruugi maksimaalselt kõiki aspekte ära katta.

Intsidentide üle arvestuse pidamine erineb asutustes suurel määral. ISKE sätestab L ja M turbetaseme korral kohustuse kõiki osapooli teavitada, kaasa arvatud CERT-EE-d, kelle pädevuses on infoturbeintsidentide analüüsimine. H taseme puhul on kohustus teavitada Riigi Infosüsteemi Ametit. Viimane saab intsidentide kohta informatsiooni ka monitooringusüsteemide vahendusel ning reeglina ei jää ükski suurem intsident tähelepanuta. Riiklikul tasemel uuritakse iga intsidenti CERT-EE poolt eraldi. Nende põhjal tehakse statistikat ja vastavalt sellele töötatakse välja suuniseid, kuidas selliseid olukordi vältida. ISKE rakendajad enamasti teostavad süsteemidele seiret, kuid ei pea arvet intsidentide üle ega tee kogutud andmete põhjal asutusesisest statistikat.

3.2.6 AUDITEERIMINE JA SELLE TULEMUSED

Auditeerimise eesmärk on hinnata ISKE rakendamise edukust. Infosüsteemide turvameetmete süsteemi määruses kirjeldatud tähtajad on nüüdseks möödunud ning on selgunud, et auditeerimise tsükkel ettenähtud kujul ei realiseeru. ISKE-t ei ole jõutud täies mahus rakendada ning auditeeritud on veelgi väiksem osa sellest.

Siiamaani läbi viidud auditite tulemused näitavad ISKE rakendamise kvaliteedi kõikumist suurel määral. Esinenud on ka juhtumeid, mil ISKE rakendamist on peetud nõuetele mittevastavaks. Suurimad puudused on seotud testimise ja avariiplaanidega – testimisi ei viida läbi ning avariiplaanid on aegunud või ei vasta olukorrale.

Ka auditeerimise vallas esineb teatud väljakutseid. Audiitorite tase on väga erinev. Mõni audiitor süveneb põhjalikult olukorda ja abistab ISKE rakendamisel, kuid leidub ka juhuseid, mil audiitor täidab järjest *checklisti* linnukestega ja lahkub.

3.2.7 ISKE-ALANE KOOLITAMINE

Riigi Infosüsteemi Amet on kodulehele kokku kogunud laialdaselt materjali ISKE rakendamise kohta. Seal on välja toodud lingid seadustele ja määrustele, standarditele, soovituslikele juhenditele ja raamdokumentide näidistele. Samuti on kodulehel ära toodud korduma kippuvad küsimused, viide ISKE rakendamist hõlbustavale tööriistale jpm [42].

ISKE valdkonnas on läbi viidud mitmeid erinevaid koolitusi Riigi Infosüsteemi Ameti poolt. Siiamaani on koolituste fookus olnud nö „mis" tasemel – koolitused on olnud suunatud juhtidele ja spetsialistidele ja nende eesmärgiks on ISKE olemuse lahtimõtestamine. Järgmisest aastast on fookus nö „kuidas" tasemel ning hakatakse läbi viima *hands-on* koolitusi, mis on mõeldud eelkõige administraatoritele ja IT-spetsialistidele.

Üheks väljakutseks on koolitajate leidmine. Teoreetilisi koolitajaid on piisavalt, kuid probleemiks on saanud praktiliste koolituste läbiviimine. Eestis on väga vähe koolitajaid, kes omavad praktilist kogemust ja ei ole juba täies töömahus seotud teiste projektidega.

Intervjueeritavad on ühel meelel, et koolitused on väga olulised ISKE rakenduskava mõistmiseks. Läbi koolituste kasvab teadlikkus ning paljudes asutustes ei ole vaikimisi kompetentsi hakata ISKE-t praktiliselt rakendama.

3.2.8 EESMÄRGID JA ARENGUPLAANID

ISKE rakendamise seisukohast on põhieesmärgiks saavutada nõutud tase terviklikkuse, konfidentsiaalsuse ja käideldavuse tagamisel ning saada edukalt auditeeritud. Toimepidevuse tagamine on otseselt seotud vabade ressurssidega. Seetõttu oodatakse ka riigilt rohkem tuge nii rahaliselt kui ka *know-how* osas.

Otseselt igapäevase toimepidevuse tagamisega seotud eesmärgid on asutustel erinevad ja sõltuvad ettevalmistatuse tasemest. Intervjueeritud ISKE rakendaja väljendas lootust uuendada lähitulevikus võrku ja toetavat infrastruktuuri, et olla paremini kaitstud looduslike riskide ja elektrikatkestuste vastu. Paljud toimepidevust tagavad asutused seisavad silmitsi probleemiga, kus uuemad lindilugejad ei pruugi enam vanemaid arhiivikoopiaid välja lugeda ning ka see aspekt vajab tulevikus lahendust.

Riiklikul tasandil on põhieesmärgiks tagada jätkuv ISKE uuendatud versioonide tõlkimine ja uute tehnoloogiate turvamine. Järgmisel aastal toimub M ja L turbetasemete eestistamine 7.0 versioonis – siiamaani oli kasutusel otsetõlge saksakeelsest standardist, milles olid viited saksa seadustele ja normidele. Plaanis on lisada ka juhendid X-tee, ID-kaardi, digiallkirja, mobiil-ID ja analoogsete lahenduste kohta.

Hetkel töötatakse Riigi Infosüsteemi Ametis välja määrust, mis kohustab suuremate riigiasutuste juhtkonda määrama infoturbe juhi. Antud positsioon planeeritakse viia kantslerite tasemele. Infoturbejuhina nähakse inimest, kes on suuteline juhtima ISKE rakendamist nii IT poolel kui ka seaduste ja määruste tasemel.

Jätkuvalt planeeritakse 2012. aastasse ISKE-alaseid koolitusi. Lobitöö suunatakse tippjuhtidele ja ülejäänud ressurss panustatakse *hands-on* koolitustesse.

Paika on pandud auditeerimise eesmärgid – 2011. aasta lõpuks peaksid olema kõik ministeeriumid end ära auditeerinud. Samuti on plaan hakata läbi viima *penetration* teste, mille käigus saadetakse eksperdid juhuvalimiga asutusse kohapealset olukorda hindama.

3.3 ELUTÄHTSAD TEENUSED

3.3.1 KIRJELDUS

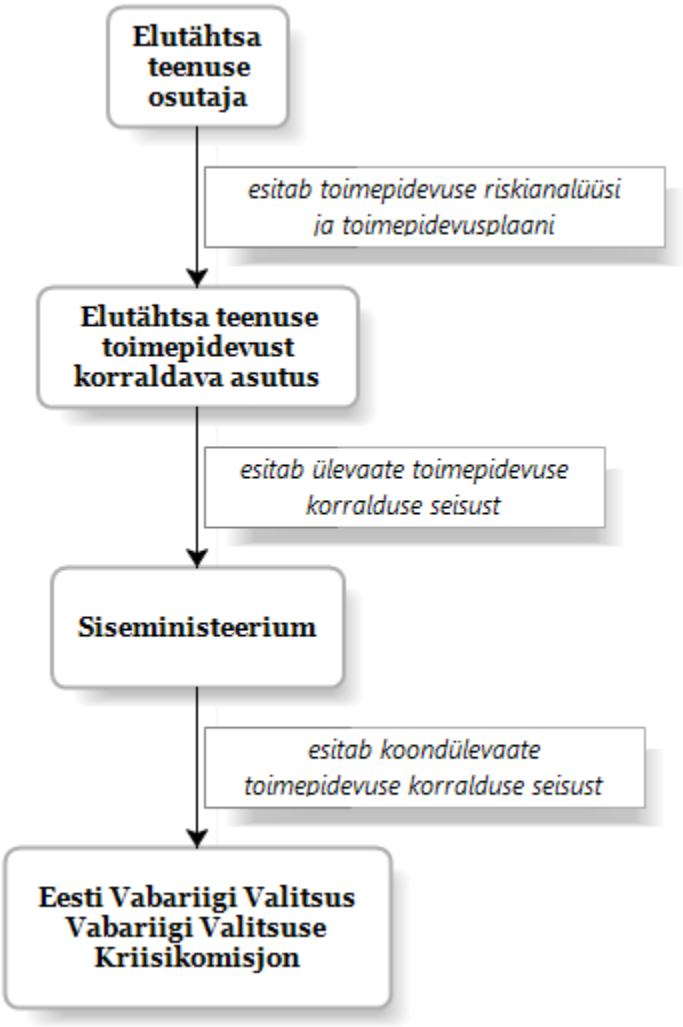
Elutähtis teenus on teenus, mis on hädavajalik eluliselt tähtsate ühiskondlike toimingute, tervishoiu, turvalisuse, julgeoleku ning inimeste majandusliku ja sotsiaalse heaolu korraldamiseks [28].

Eestis on hetkel 42 erinevat elutähtsate teenuste liiki. Elutähtsate teenuste hulka kuuluvad näiteks elektrivarustuse, andmesidevõrgu ja eriarstiabi toimimine. Aastal 2008 kaardistati kõik elutähtsate teenuste osutajad, keda on ligi 160. Teenuseid korraldavad Justiitsministeerium, Majandus- ja Kommunikatsiooniministeerium, Siseministeerium, Sotsiaalministeerium, Keskkonnaministeerium, Põllumajandusministeerium, Rahandusministeerium, Eesti Pank ja kohalikud omavalitsusüksused [1].

Elutähtsate teenuste osutajad esitavad valdkonda korraldavale asutusele ülevaate oma toimepidevuse tagamisest. Korraldavad asutused esitavad omakorda oma hallatavate elutähtsate teenuste osutajate ülevaate Siseministeeriumile, kellel on kohustus iga kahe

aasta tagant teha koondülevaade Eesti Vabariigi Valitsusele ja Vabariigi Valitsuse kriisikomisjonile [1] (joonis 2).

Riiklikul tasandil koordineerib veel elutähtsate teenuste osutajate infosüsteemide poolt vastloodud Riigi Infosüsteemi Ameti järelevalve osakond.



Joonis 2. Elutähtsate teenuste toimepidevuse tagamine ja järelevalve.

3.3.2 SEADUSLIKUD REGULATSIOONID

Eestis on elutähtsate teenuste osutajate toimepidevuse tagamine seaduslikult reguleeritud hädaolukorra seadusega [1]. Hädaolukorra seadus sätestab, et kõikidel elutähtsa teenuse osutajatel on kohustus koostada toimepidevuse riskianalüüs ja toimepidevuse plaan, mille ajakohasust tuleb hinnata vähemalt üks kord kahe aasta jooksul ja esitada iga aasta [1, 23, 28].

Hädaolukorra seaduses on ka eraldi kirjeldatud elutähtsa teenuse osutamise elektroonilise turvalisuse tagamine (§40). Selle järgi on elutähtsa teenuse osutaja kohustatud tagama elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise. Nõuded infosüsteemide turvalisusele kehtestatakse Vabariigi Valitsuse määrusega, mis hetkel veel ei eksisteeri [1].

3.3.3 TOIMEPIDEVUSE TAGAMISE ÜLEVAADE

Toimepidevuse tagamise kontseptsioon on Eestis seadusandlikul tasandil väga uus. Toimepidevuse riskianalüüsi ja toimepidevusplaani koostamise määrused jõustusid juunis 2010 ja elutähtsate teenuste osutajad olid kohustatud esimest korda vajalikud dokumendid esitama 1. jaanuariks 2011.

Praeguseks hetkeks ei ole veel kõik elutähtsate teenuste osutajad jõudnud toimepidevusplaani esitada. Esineb palju puudujääke ja esitatud plaanide kvaliteet on väga kõikuv. Elutähtsate teenuste osutajad on väga erinevad – väga väikestest ettevõtetest suurte korporatsioonideni. Mõned neist on tegelenud toimepidevuse tagamisega juba aastaid ja mõnede jaoks on tegemist täiesti uudse kontseptsiooniga. Siinkohal võib näiteks tuua suured pangad, millel on väljakujunenud kvaliteedijuhtimissüsteemid ja muud organisatoorsed poliitikad. Samuti esineb väikeseid ettevõtteid, kes tutvuvad toimepidevusega alles seadusandlikku materjali lugedes.

Edukamad toimepidevuse tagajad on suurettevõtted ja korporatsioonid, kellele on toimepidevuse tagamine oluline juba ärilistest eesmärkidest lähtuvalt. Nende hulka kuuluvad näiteks pangad ja Eesti Energia. Elektrivarustuse toimimine on elutähtis teenus, millest sõltuvad väga suurel määral ka kõik teised teenused ning seetõttu on antud ettevõttes toimepidevuse tagamisega aktiivselt tegeletud juba pikka aega. Samuti on positiivselt esile tõstetud Majandus- ja Kommunikatsiooniministeeriumi haldusalas olevaid elutähtsate teenuste osutajad.

Vähem edukad on kohalike omavalitsuste all olevad elutähtsate teenuste osutajad. Siinkohal võib olla määravaks faktoriks ka see, et ministeeriumite halduses olevad elutähtsate teenuste osutajad jäävad reeglina aastateks samaks, kohalike omavalitsuste all olevad aga muutuvad tihti. Keeruline olukord on ka Sotsiaalministeeriumi halduses olevate teenustega, eriti kiirabi ja eriarstiabi toimimise vallas. Tervishoiusektor on väga

omanäoline ja haiglad väga erineva omandivormiga, seetõttu on keeruline nõuda kõikidelt samadel alustel riskianalüüse ja toimepidevusplaane.

Vaatamata üldistele tendentsidele esineb juhtumeid, kus Eesti mõistes suur elutähtsa teenuse osutaja ei ole esitanud toimepidevusplaani, kuid vaid kaheksa kuud kohalikus omavalitsuses elutähtsat teenust osutanud ettevõte tegutseb aktiivselt riskianalüüsi ja toimepidevusplaani koostamisega. Varajased järeldused esitatud dokumentide kohta näitavad, et toimepidevuse riskianalüüse esitatakse rohkem kui toimepidevusplaane. Plaanide esitamist ei saa aga käsitleda kui ainsat toimepidevuse tagamise mõõdikut. Paljud elutähtsate teenuste osutajad on tegelenud juba pikemat aega süsteemide ja protsesside kindlustamisega teiste tööülesannete raames. Toimepidevuse aspektid on läbi mõeldud ja läbi arutatud, kuid need teadmised ei ole veel paberile jõudnud.

Hiljuti valmis Siseministeeriumis koondülevaade kõikide korraldavate asutuste materjalide põhjal. See esitati ka Vabariigi Valitsuse kriisikomisjonile.

3.3.4 TOIMEPIDEVUSE TAGAMISE VÄLJAKUTSED

Toimepidevuse tagamine seadusandlikul alusel on väga uus temaatika nii elutähtsate teenuste osutajatele, neid korraldavatele asutustele kui ka seadusandluse algatajatele. Kõik rollid ja ülesanded ei ole veel hästi paigas ja praktilisel tasemel ei ole selge, kes peaks initsiatiivi üles näitama. Esineb juhtumeid, kus korraldav asutus nendib, et elutähtsate teenuste osutajad ei ole plaane esitanud ja elutähtsate teenuste osutajad ei ole plaane esitanud, kuna korraldav asutus ei ole neid küsinud. Ka järelevalve osas on rollid hägused – korraldavad asutused jätavad tihti analüüsid ja plaanid kontrollimata, kuna neil ei ole valdkondlikke spetsialiste. Hädaolukorra seaduse sõnastust tõlgendades saab eeldada, et korraldavad asutused peaksid hindama esitatud dokumente ka sisuliselt. Siseministeeriumi ootuseks on aga see, et korraldavad asutused kontrolliks vähemalt analüüside ja plaanide vastavust juhendile.

Toimepidevuse tagamise vajaduse tunnetamine on väga erinev. Paljud intervjueeritavad on ühel meelel, et elutähtsate teenuste osutajad on mõistnud selle olulisust ning analüüsi ja plaani esitamine on vaid lisakohustus. Erandiks võib lugeda väiksemad ettevõtted ja asutused, kes on napilt täitnud elutähtsa teenuse osutaja kriteeriumid ning ei mõista, miks nende teenus on üldse elutähtis. Huvitavaks näiteks on siinkohal mõni internetiteenuse

pakkuja, kes on ületanud 1000 lõppkasutaja lävendi ja kes võib olla ainult ühe töötajaga ettevõte. Samuti leidub elutähtsate teenuste osutajaid, kes sooviksid plaani asemel täita linnukestega *checklist*i, mõistmata et toimepidevusplaani ei tehta esitamiseks vaid eelkõige iseendale paremaks kriisijuhtimiseks.

Kuigi enamik elutähtsate teenuste osutajaid näeb toimepidevuse tagamise vajadust, seab vabade ressursside olemasolu sellele piirangud. Soovitakse, et kõik põhilised toimingud saaks tehtud võimalikult efektiivselt ja väikese kuluga. Keeruline olukord on näiteks Haigekassa poolt finantseeritud haiglatel, kellele makstakse konkreetsete ravijuhtude eest. Sellisel juhul peab haigla võtma vahendeid tervishoiuteenuse arvelt, et täita riigi poolt pandud kohustusi. Toimepidevuse tagamisel kerkivad esile ka inimressursi küsimused. Tihtipeale täidetakse toimepidevuse riskianalüüsi ja toimepidevusplaani koostamise kohustust põhitöö kõrvalt, samuti on problemaatiliseks aspektiks vastava kompetentsi leidmine. Elutähtsate teenuste osutajate teadlikkus oli vähene ja enamik ei olnud varasemalt plaane teinud. Ressursipuudus on väga terav ka kohalikes omavalitsustes, kus ei leidu piisavalt spetsialiste, et esitatud dokumente kontrollida.

Kõik intervjueeritavad tõid välja, et praegused juhendmaterjalid toimepidevuse riskianalüüsi ja toimepidevusplaani koostamiseks on liiga keerulised ning ei ole üheselt arusaadavad. Samuti on raske leida universaalset metoodikat nii erinevatele ettevõtetele. Riskianalüüsis ära toodud riskid ei kata alati kõiki aspekte ära, samuti on riskimaatriksite koostamine segadusse ajav. Näiteks võib siin tuua olukorra, kus põhjalikult määrusega tutvunud ettevõte sai lõpuks valmis 211 reaga ruutmeetrisuuruse Exceli tabeli ning valminud analüüs on nii keeruline, et seda suudab täielikult mõista ainult koostaja. Samuti on teenusepõhine mõtteviis veel võõras ja nõuab harjumist.

Kõige suurem väljakutse elutähtsate teenuste toimepidevuse tagamisel on sisuliselt mõista, mis on elutähtis teenus. 2008. aastal kaardistati küll kõik elutähtsa teenuse osutajad, kuid hetkel ei ole kaardistatud elutähtsad teenused. Seaduses on olemas elutähtsa teenuse üldine definitsioon, kuid reaalsuses kuuluvad elutähtsate teenuste valdkonda teenused, mis ei pruugi olla elutähtsad ning mitmed potentsiaalselt elutähtsad teenused on praeguse liigituse järgi välja jäänud. Siinkohal saab näiteks tuua andmesidevõrgu toimimise. Ühed suurimad elutähtsate teenuste osutajad on selles valdkonnas Elion ja EMT. Antud ettevõtted pakuvad telefonisideteenust, SMS-teenust, Internetti, digiTV-d jt teenuseid. Võib nõustuda, et telefoniside toimimine on elutähtis teenus, kuid jääb selgusetuks, kas elutähtis on ka

näiteks digiTV või SMS-i saatmise võimalus. Mitmed elutähtsate teenuste osutajad pakuvad erinevaid alamteenuseid. Siinkohal on toimepidevuse tagamine väga tugevas seoses äriliste eesmärkidega – paremini turvatakse neid süsteeme, mis rohkem kasumit toovad.

3.3.5 VALDKONDLIKU TOIMEPIDEVUSE TAGAMINE

Elutähtsate teenuste osutajate toimepidevuse tagamise kõrval on oluliseks aspektiks ka valdkondliku toimepidevuse tagamine. Siseministeeriumis valminud koondülevaate põhjal hakatakse kaardistama sõltuvusi valdkondade vahel. Hetkel eksisteerib 5-6 valdkonda, millest sõltuvad kõik ülejäänud. Raske on otsustada, kuhu panustada rohkem ressursse, kuna indiviidi ja riigi vaade teenuste tähtsusest on üsna erinev. Näiteks hindavad paljud tavaisikud kiirabi ja pääste toimimist väga oluliseks, kuid ei pane tähtsate teenuste sekka põhi- ja tugimaanteede või teede ja linnatänavate toimimist. Indiviid ei hooma, et kui teedevõrk ei toimi, siis ei ole võimalik ka kiirabil kuidagi abivajajani jõuda. Samuti on riigil raske hallata teatud kriitilisi valdkondi. Näiteks veevarustuse pakkujaid on viis erinevat ning nad kuuluvad kõik erinevate korraldavate asutuste alla.

Eraldi väljakutseks on tagada valdkondlik toimepidevust olukorras, kus riigi ja elutähtsate teenuste osutajate toimepidevusalased eesmärgid on vastandlikud. Siinkohal võib tuua näite, mis on seotud katkestuse ajastusega. Riigile on väga kahjulik, kui neli suuremat panka korraga ei toimi, kui pankade vaatepunktist on äririskid maandatud – kõik neli on võrdsel positsioonil.

Ministeeriumid ja kohalikud omavalitsused on hinnanud elutähtsate teenuste võimekust valdkonniti. Eksisteerivad teatud tegevusvarud ja on läbi mõeldud, keda esimesena teenindada kriisiolukorras. Suures plaanis seisavad aga korraldavad asutused silmitsi riigile sarnaste probleemidega.

3.3.6 IT-SÕLTUVUS

IT-st on saanud keskne tugiprotsess, mis toetab kõiki sisulisi protsesse. Oleme jõudnud tehnoloogiliselt arengult punkti, kus ilma infosüsteemideta protsessid enam ei toimi. Bussigraafikute planeerimine käib infosüsteemis, veevärkidel ja katlamajadel on kogu

teenuse osutamine infotehnoloogilistele juhtimissüsteemidele üles ehitatud, prügivedajatel ja tänavapuhastajatel on autodes GPS-süsteemid ning ka tänavavalgustussüsteemid toimivad IT-lahendustel.

Sõltuvus on väga suur ka seetõttu, et üha enam on vajadus monitooringu järele. Seirevajadus on nii väikestel kui ka suurtel ettevõtetel – samamoodi nagu on pankadel kohustus registreerida iga tehing, peab ka prügifirma olema võimeline kliendile tegema väljavõtte, millisel kellaajal prügiauto konteinerit tühjendamas käis. Igast tegevusest peab maha jääma kohustuslik jälg infosüsteemis.

2011. aastal alustas Riigi Infosüsteemi Amet kriitilise informatsiooni infrastruktuuri kaardistamist elutähtsaid teenuseid osutavates ettevõtetes ja asutustes, eesmärgiga saada ülevaade, kui palju kasutatakse infosüsteeme. Kaardistuseks kasutati USA-s välja töötatud *checklist*i, mille põhjal on võimalik hinnata IT-sõltuvuse taset. Hetkel on kaardistatud ligi 100 ettevõtet ja kogutud andmeid hakatakse kasutama sisendina uue järelvalveosakonna töös, mille eesmärgiks on teostada järelevalvet elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise üle, riigivõrgu tehnilise toimivuse üle ning riigiasutuste infosüsteemidele rakendatavate turvameetmete üle [47].

Sarnaselt ISKE rakendajatele on kõik elutähtsate teenuste valdkonna esindajad ühel meelel, et IT-sõltuvus kasvab lähiaastatel oluliselt. Välja on kuulutatud riigihanked uutele reaalajas süsteemidele ning olemasolevaid protsesse automatiseeritakse üha enam IT-lahenduste abil. Olulist IT-sõltuvuse kasvu võib täheldada ka tervishoiusektoris – hetkel potentsiaalsed pikaajalisemad infosüsteemide katkestused veel kellegi elu ohtu ei sea, kuid hinnanguliselt muutuvad hiljemalt 2-3 aasta pärast süsteemid juba kriitilisemaks.

3.3.7 RISKIDE MAANDAMINE

Riskide maandamise osas on elektrivarustuse tagamine tänapäeval toimepidevuse aspektist esimene ja kõige tähtsam kriteerium. Elutähtsate teenuste osutajad investeerivad varugeneraatoritesse ja UPS-idesse. Infosüsteemid on dubleeritud, mõni isegi kuni neljakordselt.

Väga palju pööratakse tähelepanu varukoopiate tegemisele. Kuigi üldhinnang näitab, et varukoopiate tegemisel on arenguruumi, eriti varukoopiate eraldi hoidmises ja neist taastamise testimisel, kinnitasid kõik intervjueeritud toimepidevust tagavad asutused, et kogu varundusprotsess on väga detailselt reguleeritud ja 100%-liselt töös.

Vähem mõeldakse uute tehnoloogiate turvamisele, näiteks nutitelefonide ja tahvelarvutite kindlustamisele. Samuti alahinnatakse väga väikese tõenäosusega riske, näiteks üleujutusi ja kiirgust.

Riiklikul tasemel riskianalüüsis on väga kõrge riskiga hinnatud küberrünnaku ohtu [48]. Koostatud on hädaolukorra lahendamise plaan, mis on suunatud elutähtsate teenuste osutajatele. Küberrünnaku ennetamise meetmed peaksid olema kirjeldatud vastavas infosüsteemide turvameetmete määruses, kuid seda veel ei eksisteeri.

Suureks valupunktiks ennetamisel on toimepidevusplaanide testimine ja harjutuste läbi viimine. Toimepidevusplaani koostamise juhend sätestab, et kõikidel elutähtsate teenuste osutajatel on kohustus läbi viia regulaarseid harjutusi, kuid regulaarsus jääb ettevõtte või asutuse enda otsustada. Eksisteerib seaduspärasus, et need, kes korraldasid juba varem harjutusi, jätkavad nende tegemist. Positiivselt saab esile tõsta energeetika- gaasi, lennundus-, raudtee- ja laevaliikluse valdkonnad ning äriliste eesmärkidega ettevõtted. Mitmed ülejäänud elutähtsate teenuste osutajatest ei ole harjutusi töökavasse võtnud ka peale hädaolukorra seaduse jõustumist.

Paljudel korraldavatel asutustel puudub ülevaade testide tegemise kohta ja intervjueeritud asutused tunnistasid, et teste praktiliselt läbi ei viida. Seda juhtub eriti IT-valdkonnas. Mõni neist on teadvustanud harjutuste vajalikkust, kuid ei ole jõudnud veel ühtegi teha. Ülejäänud ei tee teadlikult, kuna ei ole piisavalt finantsvahendeid, et ehitada paralleelsüsteem, kus simuleerida probleeme. Tehtud on ettepanekuid, et järelevalve korraldajad võiks ka ise korraldada valdkonna sees teste. Hetkel tehakse Küberkaitseliidu poolt küberteste ja valimisse satuvad mõnikord ka elutähtsate teenuste osutajad.

Vaatamata vähestele toimepidevusplaani harjutustele on kõikides intervjueeritud asutustes määratud kriisijuhid ja -meeskonnad, kes on toimepidevuse alased aspektid aastatepikkuses praktikas läbi mõelnud.

3.3.8 KATKESTUSED JA NENDE HALDUS

Kõik intervjueeritavad hindavad üldist olukorda heaks. Ei eksisteeri ühtegi elutähtsat teenust, mille katkestus on kestnud üle paari päeva. Paraku ei ole võimalik adekvaatselt hinnata, kas riskid on hästi maandatud või on tegemist õnneliku juhusega.

Tänapäeval on tüüpilisemad katkestused tingitud tehnilistest riketest ja inimvigadest. Kõige sagedamini esinevate katkestustena toodi välja elektrikatkestusi, infosüsteemide uuendustest tingitud ettenägematuid viivitusi ja serverite tehnilisi rikkeid. Ükski eelmainitud katkestus ei ole endaga kaasa toonud kriitilisi tagajärgi ega arenenud suuremahulisemaks kriisiks. Järgmine suurem grupp katkestusi on valdkonnaspetsiifilised, näiteks ühistranspordi ja jäätmekäitluse toimimist on viimastel aastatel mõjutanud rängad lumeolud.

Elutähtsate teenuste osutajatel on kohustus teavitada oluliselt häirivast sündmusest või sellise sündmuse toimumise vahetust ohust [1]. Taolisi suure mõjuga sündmusi on esinenud vähe. Tavaliste intsidentide üle arvepidamine erineb asutuseti suurel määral. Esineb elutähtsa teenuse osutajaid, kes teevad päeva-, nädala-, kuu- ja aastaanalüüse ning teavitavad korraldavat asutust igast rikkest juba lepingulistest kohustustest tulenevalt. Samuti esineb ettevõtteid, kes peavad intsidentide üle registrit oma ainult oma tarbeks. Korraldavad asutused määravad intsidentide halduse korra ise. Ei ole välja kujunenud ühtset metoodikat registreerimiseks ega kategoriseerimiseks raskusastmete järgi. Üldist riiklikul tasemel korrastatud andmekogu ei eksisteeri.

Riigi Infosüsteemi Ameti eestvedamisel on arendatud süsteem nimega virtuaalne situatsiooniruum. Süsteemi ei ole veel kasutustele võetud, kuna selle eesmärk ei ole selge ja paljud sellega seotud küsimused ootavad veel lahendust. Määramata on kas virtuaalne situatsiooniruum on mõeldud kriisijuhtimiseks või monitooringuks, samuti ei ole kindel, millist infot peaksid elutähtsate teenuste osutajad süsteemile edastama. Projektil ei ole õiguslikku alust ega määratud info omanikku. Süsteemi eesmärkideks on pidada arvet intsidentide üle riiklikul tasandil ja andmeid üldistatud moel jagada. Hetkel on situatsiooniruumil lahendamata ka teatud ärilistest aspektidest tulenevad probleemid. Kuna on selgusetu, kuidas kaitstakse kõikide osapoolte huvisid, ei ole paljud ärijuhid huvitatud intsidentidest teavitamisest, sest konkurendid võivad neid teadmisi ära kasutada.

3.3.9 TOIMEPIDEVUSE ALANE KOOLITAMINE

Juba toimepidevuse tagamise väljakutsete alampeatükis toodi välja, et riskianalüüsi ja toimepidevusplaani koostamise juhendid on elutähtsate teenuste osutajate jaoks liiga keerulised. Seadus sätestab, et korraldavad asutused nõustavad vajaduse korral oma haldusalas olevaid teenuseosutajaid. Intervjuudest selgub, et korraldavad asutused on abistanud oma elutähtsate teenuste osutajaid seadusandliku materjali ja sellega seotud tähtaegade välja otsimisega. Samuti on korraldatud kriisikoosolekuid, kus erinevad teenuseosutajad saavad omavahel kogemusi vahetada ning koos korraldava asutusega riskianalüüse ja toimepidevusplaane läbi vaadata. Paraku ei ole viimasel tihtipeale piisavalt spetsialiste, et sisuliselt toimepidevuse tagamisel aidata.

Toimepidevuse osas on koolitusi vähe läbi viidud. Siseministeeriumi eesmärgiks on koolitada valdkondi korraldavaid asutusi, kes omakorda koolitavad elutähtsate teenuste osutajaid. Koolitusprotsess on olnud puudulik igast vaatenurgast – omavalitsused ja ministeeriumid ei ole näidanud üles väga palju initsiatiivi koolituste korraldamisel, samuti esineb juhtumeid, kus elutähtsa teenuse osutaja tunnistab, et tiheda töökava tõttu unustati koolitusele minna. Riigi Infosüsteemi Amet viis läbi mõned koolitused, kuid esitatud plaanide kvaliteet oli sellele vaatamata kohati nõrk.

3.3.10 EESMÄRGID JA ARENGUPLAANID

Kõige suuremad muudatused viiakse läbi hädaolukorra seaduse osas. Lähiajal valmis Siseministeeriumis seaduse analüüs, mis tõi välja erinevad kitsaskohad. Hetkel on muudetud variandi väljatöötamisel aktiivsed Siseministeerium, Riigi Infosüsteemi Amet, ja elutähtsaid teenuseid korraldavad asutused. Järgmisel aastal on plaanis kirjeldada detailsemalt elutähtsate teenuste kriteeriume ning muuta toimepidevuse riskianalüüsi ja toimepidevusplaani koostamise juhendeid. Sarnase initsiatiiviga on välja tulnud päästeteenistus, kes astub samme ja on kavandanud tegevusi toimepidevusplaani juhendi lihtsustamiseks. Riskianalüüsi osas kaalutakse Prantsusmaalt pärit valdkondliku ohukaardi ideed – muuta riskide loetelu nii, et saaks konkreetsele valdkonnale anda ette spetsiifilisemad variandid.

IT-alastest muudatustest on olulisemad seotud Riigi Infosüsteemi Ameti volitustega – plaanitakse seadusesse lisada eelmainitud asutuse infoküsimise ja järelvalveõigused.

Valdkondliku toimepidevuse tagamiseks on kavandatud erakorraline hädaolukorra seaduse muudatus, millega saadetakse valitsusse serveri asukoha eelnõu.

Samuti muudetakse teenuste nimekirja – teatud teenused eemaldatakse või ühendatakse. Näiteks praegu on seaduses eraldi teenusena välja toodud jäämurdetöö toimimine, kuid edaspidi kuulub see sadamate toimimise alla. Viiakse läbi mõned terminoloogilised muudatused, näiteks õhuseire muutub lähiõhuseireks.

Lisaks eelmainitutele on Siseministeeriumi eesmärgiks järeltoimingutena saada kätte esitamata dokumendid. 2012. aasta teisel poolel hakatakse tegelema uue ülevaatusringiga. Teenuseid korraldavate asutuste eesmärgid on selles osas analoogsed Siseministeeriumile.

Riigi Infosüsteemi Ameti põhieesmärgiks on täies mahus tööle saada vastloodud järelevalve osakond. Plaanitakse välja töötada elutähtsate teenuste osutajate infosüsteemide turvameetmete nõuded. Kui asutus saab seadusliku infoküsimise õiguse, hakatakse laialdasemalt koguma ja hindama elutähtsate teenuste osutajate infosüsteemide toimepidevusplaane. Samuti on eesmärgiks saavutada rohkem personaalset kontakti elutähtsate teenuste osutajatega.

Aina teravamalt nähakse vajadust täpsustada elutähtsate teenuste kriteeriume. See on ülesanne, mille täitmise kohustus langeb tõenäoliselt korraldavatele asutustele koostöös teenuseosutajaga. Kindlaid plaane protsessi läbi viimiseks veel ei ole.

3.4 VALITUD NÄITEID TOIMEPIDEVUSEGA SEOTUD INTSIDENTIDEST EESTIS VIIMASTEL AASTATEL

3.4.1 DIGIRETSEPTI SÜSTEEMI KÄIVITAMINE

3.4.1.1 Kirjeldus

Digiretsept on üks osa eesti riigi e-tervise projektist. Digiretsepti all mõistetakse elektroonilist ravimiretsepti, mille arst patsiendile arvutis valmis kirjutab. Digiretsepti ei trükita paberil välja, vaid saadetakse arsti arvutist interneti teel otse retseptikeskusesse. [49].

Apteeki minnes peab ravimi väljaostjal olema kaasas enda isikut tõendav dokument, kus on peal pilt ning isikukood, näiteks ID-kaart, juhiluba või pass. Apteeker leiab retseptikeskusest patsiendi isikukoodi abil hõlpsasti üles kogu talle vajaliku info [49].

Digiretsepti süsteemile mindi üle 1. jaanuaril 2010. Kuni 28. jaanuarini 2010 kehtis üleminekuperiood, mille vältel võisid arstid välja kirjutada nii paber- kui ka digiretsepte. Peale antud kuupäeva oli ette nähtud täiemahuline üleminek digiretseptide kirjutamisele, välja arvatud erijuhtudel nagu näiteks koduvisiidid või elektrikatkestus [50].

3.4.1.2 Intsidendid

Maksimaalne planeerimata katkestus digiretsepti töös võib olla kuni 15 minutit [51]. Üleminekuperioodil ja peale seda tekkis mitmeid katkestusi, mis kestsid tunduvalt kauem kui ettenähtud ajavahemik.

5. jaanuaril 2010 tekkisid segadused ravimite soodustusega, kuna süsteem ei lubanud soodustust valida ja parandada [52].

13. jaanuaril 2010 tekkis digiretseptikeskuse andmebaasi rike [53].

21. jaanuaril 2010 tõrkusid digiretsepti süsteemi serverid taas [54].

3. veebruaril 2010 tekkis ühe tunni ja 10 minuti pikkune katkestus, mille vältel ei saanud digiretsepte retseptikeskusesse saata ja neid sealt vaadata [55].

Märtsikuu alguse pensioni- ja palgapäevadel ajal selgus, et süsteem ei pea vastu suurenenud koormusele ja tõrgub töötamast [56].

1. aprillist kuni 12. aprillini 2010 oli digiretsept igal päeval tundide kaupa maas, kuna süsteem ei suutnud toime tulla sellele pandud koormusega [57].

12. novembril 2010 oli digiretseptide väljastamine mitu tundi häiritud [58].

8. märtsil 2011 ilmnesid digiretsepti süsteemis taas tõrked [59].

3.4.1.3 Tagajärjed

Digiretsepti süsteemi tõrgete tõttu olid häiritud arstid, patsiendid ja apteekrid. Arstid ei saanud süsteemi maasoleku ajal digiretsepte kirjutada, apteekrid neid väljastada ning patsiendid ravimeid välja osta. Sealhulgas jäid operatiivsest teenindusest ilma kliendid, kelle jaoks oli kriitiline saada ravimid kätte ettenähtud kitsa ajavahemiku jooksul, näiteks valuvaigistite vajajad ja haigete väikelaste hooldajad [52, 53, 54, 55, 56, 57, 58, 59].

Samuti mõjusid korduvad katkestused halvasti digiretsepti süsteemi mainele. Pettumust avaldas teiste seas avalikus meedias ka peaminister Andrus Ansip [60].

3.4.1.4 Talitluspidevuse tagamiseks kasutusele võetud meetmed

Kriiside leevendamiseks võeti kasutusele erinevaid meetmeid. Arstidel paluti kirjutada paberretsepte [55] ja asuti suurendama süsteemi võimsust [61]. Juba digiretsepti saanud patsientide teenindamiseks oli võimalik helistada operaatorile ja üritada retsepti broneerida [53]. Mõned apteekrid otsisid kliendile käsimüügist asendusravimi või andsid retseptiravimi suulise kokkuleppe peale [53]. Jääb selgusetuks, kas viimased meetmed olid kooskõlastatud talitluspidevuse tagamise tegevus või apteekrite isiklik abinõu kriisi leevendamiseks.

Süsteemi võimsusi asuti kohe ümber projekteerima, kuid see viibis ja tõrkeid on esinenud rohkem kui aasta peale süsteemi kasutuselevõttu. Sellegipoolest on praeguseks enamik kitsaskohtadest likvideeritud ja rohkem ei ole suuremaid katkestusi esinenud.

3.4.2 VALIMISTULEMUSTE KUVAMINE

3.4.2.1 Kirjeldus

6. märtsil 2010 toimusid Eestis riigikogu valimised. Sama päeva õhtul hakati valimistulemusi kuvama internetis valimistulemuste infosüsteemi avaliku liidese kaudu. Valimisandmete edastamisel internetis tekkis viivitus [62].

3.4.2.2 Intsident

6. märtsi õhtul avastati, et valimistulemused ei ole uuenenud. Valimistulemuste andmebaasis oli viga, mis nõudis korduvat rakendusserveri algkäivitust. Süsteem saadi töökorda 1,5 tundi hiljem. Lepingujärgselt oli lubatud infosüsteemi mittetoimimise aeg 15 minutit [63].

3.4.2.3 Tagajärjed

Inimestel puudus võimalus jälgida valimistulemuste saabumist reaalajas. Intsident seadis löögi alla riigikogu valimiste usaldusväärsuse [64]. Samuti mõjusid infosüsteemi loonud Helmes AS tegevjuhi Jaan Pillesaare kriisijärgsed sõnavõtud halvasti eelmainitud firma mainele [65]. Vastavalt auditi tulemustele oli AS Helmes kohustatud maksma 8503 eurot leppetrahvi [66].

3.4.2.4 Talitluspidevuse tagamiseks kasutusele võetud meetmed

Kriisi vahetul ilmnemisel üritati olukorda lahendada logifailide uurimisega ja rakendusserveri algkäivitamisega, mis võttis aega 1,5 tundi ettenähtud 15 minuti asemel. Auditi tulemustest selgus, et AS Helmese poolne intsidendihaldus ei olnud koordineeritud. Potentsiaalsed riskid ei olnud kaardistatud. Vabariigi valimiskomisjoni ja AS Helmese esindajatest oli moodustatud kriisiohjamismeeskond, kuid puudusid detailsed tegevusjuhised ja riskiplaanid. Vabariigi Valimiskomisjonil eksisteeris äririski maandamiseks varuplaan, kuid selle käikuandmisega viivitati, sest AS Helmes kinnitas Vabariigi Valimiskomisjoni esindajale kogu intsidendi jooksul probleemi peatset lahendumist [63].

3.4.3 EESTI ENERGIA KLIENDIINFOSÜSTEEMI TÕRKED

3.4.3.1 Kirjeldus

Aprillis 2011 käivitus uus Eesti Energia kliendiinfosüsteem, mis võtab vastu igakuiseid elektrinäite. Läbi antud süsteemi esitab andmeid ligi pool miljonit klienti [67].

3.4.3.2 Intsident

Süsteemi käivitumisel esines tõrkeid, mille tõttu ei saanud mitmed kliendid elektrinäitu esitada [68]. Häiritud oli eelkõige e-teenindus ja näidu teatamine SMSiga. Samuti olid pikad järjekorrad infotelefonil 1545 [69].

3.4.3.3 Tagajärjed

58 000 klienti, kes ei saanud mingil põhjusel näitu esitada või tegid seda liiga hilja, said prognoosarve. Ligi 7000 klienti said aprilli arve hilinemisega koos maikuu arvega juunis [68].

3.4.3.4 Talitluspidevuse tagamiseks kasutusele võetud meetmed

AS Eesti Energia avaldas 30. aprillil pressiteate, kus hoiatas võimaliku ülekoormuse eest ja palus klientidel eelistada prognoosnäitu [67]. Kogu tõrgete perioodi vältel andis Eesti Energia operatiivselt infot näitude esitamise süsteemi oleku kohta ja andis klientidele tegevusjuhiseid [67, 68, 70]. Süsteem häälestati vastavalt koormusele ja nüüd töötab see ettenähtud mahus.

3.4.4 ELIONI JA EMT TUUMIKVÕRGU RIKKED

3.4.4.1 Kirjeldus

Elion on üks suurimaid Eesti telekommunikatsioonieettevõtteid, mille pädevuses on internetiühenduse, telefoniside ja digiTV pakkumine üle Eesti.

3.4.4.2 Intsidendid

17. novembril 2010 kell 10.45 avaldusid probleemid Elioni teenuste toimimisega, mis puudutasid nii Elioni digiTV, interneti kui ka VoiP telefoni kliente üle Eesti [71]. Katkestuse pikkuseks oli 1 tund ja 15 minutit [72]. Katkestuse põhjuseks oli Elioni tuumikvõrgu rike [73].

1. detsembril 2010 tekkis uus tuumikvõrgu rike, mille tõttu oli 1,5 tunni jooksul häiritud mobiilsideühendus [74].

3.4.4.3 Tagajärjed

Interneti tuumikvõrgu rikke tõttu olid häiritud kaupluste kaardimaksed, pankade sularahaautomaatide töö ning osa pangakontorite ja reisifirmade check-in'ide tegevus. Võrguprobleemide tõttu kannatas EMT 3G-võrgu ühendus [75]. Samuti ei saanud Elioni kliendid lauatelefonilt helistada hädaabinumbrile 112 [76].

EMT tuumikvõrgu rikke tõttu oli häiritud 750 000 kliendi mobiilside [74].

3.4.4.4 Talitluspidevuse tagamiseks kasutusele võetud meetmed

Probleemi lahendamisega tegeleti operatiivselt ja plaanikohaselt. Probleem lahendati kiirelt ja kliente teavitati tegevusplaani järgi. Samuti tegeles Elion intsidendijärgselt põhjalikult juhtumianalüüsiga, et edaspidi sarnaseid situatsioone vältida [73].

Elion tegi täiendavad plaanid taolise juhtumi välistamiseks tulevikus ja suurendas investeeringuid tuumikvõrku. Samuti võeti plaani Elioni teenuste ja võrgu arhitektuuri põhjaliku analüüsi teostamine [77].

EMT tuumikvõrgu rikke osas tegutseti samuti plaanipäraselt. Vigane seade lokaliseeriti ja häiritud tuumikvõrgu osa isoleeriti operatiivselt vastavalt kehtestatud reeglitele. Juba varasemast on kogu EMT tuumikvõrk dubleeritud, jaotatud erinevateks teenindavateks kihtideks vastavalt parimale tehnoloogilisele tavale ning üle dimensioneeritud eriolukordade paremaks talumiseks [78].

Sarnaselt Elioni rikkele võttis EMT plaani analüüsida võrguarhitektuuri ja süsteemide täiendava dubleerimise võimalusi [78].

4 TÄHELEPANEKUD JA JÄRELDUSED

Riigi Infosüsteemi Ameti 2011. aasta koolitusprogramm kannab ettenägelikult nime „Tark e-riik". Selle raames on korraldatud nii ISKE-alaseid koolitusi kui ka infopäevi, mille fookuseks on elutähtsate teenuste toimepidevus [79]. Sellegipoolest näitab intervjuude põhjal läbi viidud analüüs, et toimepidevuse tagamise vallas on jätkuvalt arenguruumi – see ei ole praegu jõudnud samale tasemele uute suurel määral infotehnoloogilistel lahendustel põhinevate teenuste loomisega.

Antud magistritöö autor toob järgnevalt läbi viidud intervjuude põhjal välja peamised tähelepanekud.

ISKE-ga reguleeritud teenused:

1. ISKE rakendamise kohustust reguleeritakse mitmes erinevas seaduses ja määruses ning aeg-ajalt tekib küsimus, millisele konkreetsetele andmekogule on vaja ISKE-t rakendada.
2. ISKE-t ei ole jõutud täies mahus rakendada ja auditeerimise tsükkel seaduses ettenähtud kujul ei realiseeru.
3. Kõige paremini on ISKE rakendatud avaliku teenuse osutajate valdkondlikes infotehnoloogia keskasutustes ja kõige rohkem puudujääke esineb omavalitsustes.
4. Peamised põhjused, miks ISKE-t ei ole rakendatud, on ressursside puudumine (rahalised vahendid, kompetents) ja selle madal prioriteet põhitegevuste kõrval.
5. ISKE uued versioonid jõuavad eesti keeles rakendajateni hilinemisega ja seetõttu ei ole kõik uued tehnoloogilised ohud alati kaetud.
6. Suurim osa katkestustest viimastel aastatel on seotud käideldavusega.
7. Kõige tüüpilisemad katkestuste põhjused on infosüsteemide arhitektuurivead, kolmandatest osapooltest põhjustatud probleemid ja mitme halva asja kokkusattumus.
8. Katkestuste üle arvet pidamine on erinevates asutustes ebaühtlane.

9. Auditeerimine on näidanud, et suurimad puudused esinevad testimise ja avariiplaanide osas.
10. Audiitorite tase on kõikuv.
11. Riigi Infosüsteemi Amet on loonud ISKE rakendajatele ülevaatliku veebilehe, kus on lingid seadustele, juhenditele, raamdokumentide näidistele, korduma kippuvad küsimused ja ISKE rakendustööriista programm.
12. ISKE rakendajatele on läbi viidud mitmeid koolitusi.
13. Eestis on vähe häid ISKE koolitajaid, kellel on praktiline rakendamise kogemus.

Elutähtsad teenused:

1. Hetkel on Eestis 42 elutähtsate teenuste valdkonda ja ligi 160 elutähtsate teenuste osutajat. Elutähtsate teenuste osutajad on väga erinevad suuruse, äriliste eesmärkide ja praktikate poolest.
2. Hädaolukorra seadus sätestab, et elutähtsate teenuste osutajad peavad üks kord kahe aasta jooksul ajakohasust hindama ja iga aasta esitama toimepidevuse riskianalüüsi ja toimepidevusplaani.
3. Hädaolukorra seaduses on kirjas, et elutähtsate teenuste osutajad peavad rakendama turvameetmed infosüsteemidele, mis on kirjeldatud vastavas määruses, kuid seda määrust veel ei eksisteeri.
4. Toimepidevuse tagamine seadusandlikul tasandil on uus kontseptsioon – määrused toimepidevuse riskianalüüsi ja toimepidevusplaani koostamiseks jõustusid suvel 2010 ja esimest korda oli vaja vastavad dokumendid esitada 1. jaanuaril 2011.
5. Praeguseks hetkeks ei ole kõik elutähtsate teenuste osutajad veel toimepidevusalaseid dokumente esitanud ning koostatud plaanide kvaliteet on väga kõikuv.
6. Edukamad elutähtsate teenuste osutajad on suurkorporatsioonid. Nõrgemad on omavalitsuste halduses olevad ettevõtted.
7. Paljud elutähtsate teenuste osutajad on tegelenud juba pikemat aega süsteemide ja protsesside kindlustamisega teiste tööülesannete raames, kuid neid tegevusi ei ole

süstemaatiliselt läbi analüüsitud ja dokumendina vormistatud. Asutused on enamasti määranud kriisijuhid ja kriisimeeskonnad.

8. Rollid toimepidevuse tagamise ja selle järelevalve osas ei ole veel ammendavalt paika saanud.

9. Teatud omavalitsustel ja ministeeriumitel ei ole piisavalt ressurssi ja kompetentsi, et sisuliselt aidata ja järelvalvet teostada.

10. Praegu kehtivad toimepidevuse riskianalüüsi ja toimepidevusplaani koostamise juhendid on ühelt poolt liiga keerulised ja teisalt ei kata kõiki spetsiifilisi asjaolusid ning ei sobi seetõttu üheselt kõigile 160 asutusele ja ettevõttele.

11. Elutähtsate teenuste kriteeriumid ei ole piisavalt detailselt määratletud.

12. Valdkonna kui terviku toimepidevuse tagamine on keeruline väljakutse. Esineb olukordi, kus sama valdkonna teenuseosutajad on erinevate korraldavate asutuste halduses ja mõnikord on riigi ja teenuseosutajate eesmärgid vastandlikud.

13. Tänapäeval kasutavad peaaegu kõik teenuseosutajad igapäevatöös infotehnoloogilisi süsteeme ja sõltuvus nendest kasvab järgmiste aastate jooksul oluliselt.

14. Kõige rohkem tähelepanu pööratakse kaitsele elektrikatkestuste vastu ja varukoopiate tegemisele, aga need protsessid ei ole täielikult läbi mõeldud. Vähem pööratakse tähelepanu uute tehnoloogiate turvamisele ja väga väikese tõenäosusega riskidele, näiteks üleujutustele ja kiirgusprobleemidele.

15. Toimepidevusplaani testimisi ja harjutusi viiakse läbi väga vähe.

16. Üldine olukord on siiamaani olnud hea - elutähtsate teenuste vallas ei ole olnud ühtegi katkestust, mis kestaks üle paari päeva ja toonud endaga kaasa väga suure mõjuga tagajärgi.

17. Kõige tüüpilisemad katkestused on olnud tingitud tehnilistest riketest ja inimvigadest.

18. Katkestuste üle arvet pidamine on ebaühtlane – igaühel on oma metoodika ja mõni asutus ei registreerigi intsidente.

19. Valminud on süsteem nimega Virtuaalne situatsiooniruum, kuid sellega on seotud lahendamata küsimusi ja sellisel kujul ei saa seda täismahus tööle võtta.

20. Toimepidevuse alast koolitamist on siiamaani olnud vähe.

Antud tähelepanekute põhjal on võimalik teha järgmised üldistatud järeldused:

1. **Toimepidevusealane teadlikkus on madal.** Tegeletakse pigem tagajärgede likvideerimisega kui ennetamisega. Tihti ei mõisteta analüüside ja plaanide koostamise ega harjutuste läbiviimise vajadust. Rollid ei ole ammendavalt paigas ja elutähtsate teenuste osas on koolitamisprotsess olnud puudulik.

2. **Toimepidevuse tagamine on otseses seoses rahaliste ressursside ja äriliste eesmärkidega.** Paremini turvatakse süsteeme, mis on kasumlikumad. Kui rahalisi ressursse on vähe (näiteks riigiasutustes ja omavalitsustes), siis on toimepidevuse tagamine muude tegevuste kõrval madala prioriteediga.

3. **Enamik avalikke teenuseid on tugevas sõltuvuses infosüsteemidest.** Paraku puudub hetkel hädaolukorra seadusest määrus, mis sätestab infosüsteemide turvameetmed. Samuti eksisteerib olukordi, kus IT osakaal aina suureneb, kuid vastav eelarve väheneb. Infotehnoloogiliste lahenduste ebapiisav turvamine on samuti seotud teadlikkusega – ei mõisteta kui suurel määral sõltuvad põhiprotsessid IT toest.

4. **Toimepidevuse tagamise kohustust sätestavad seadused tekitavad segadust.** ISKE rakendamise kohustus on jagatud erinevatesse määrustesse ja kasutatavad terminid ei määratle üheselt rakendusala. Hädaolukorra seadusega pandud tähtajad on sisuliselt ebaloogilised, juhendid liiga keerulised ja teenusevaldkondade määratlus vajab täpsustamist. Puudub eelmainitud elektroonilise turvalisuse määrus.

5. **Analüüsi ja kaardistamise osa on puudulik.** Elutähtsate teenuste kriteeriumid ei ole detailselt välja toodud ja tihtipeale ei ole kindel, milline ettevõtte kümnest alamteenusest on elutähtis. Samuti on veel ammendavalt kaardistamata sõltuvused valdkondade vahel. Intsidentidest teavitamine ja katkestuste registreerimine on ebaühtlane, samuti tehakse kogutud info põhjal vähe analüüsi, et sellest järeldusi teha ja ennetavatesse tegevustesse panustada.

5 ETTEPANEKUD

Antud magistritöö autor teeb intervjuudest saadud ülevaate põhjal järgmised ettepanekud toimepidevuse tagamise edendamiseks.

1. Tõsta toimepidevusealast teadlikkust.

Intervjuudest on selgunud, et toimepidevuse alase teadlikkuse tase on kõikuv ja üldistavas vaates jätkuvalt madal. Seetõttu on oluline läbi viia koolitusi erineval tasemel – tippjuhtkonnale ja spetsialistidele, teoreetilisi ja praktilisi.

Tähtis on teha kättesaadavaks piisaval määral selget juhendmaterjali – olemust tutvustavaid brošüüre, juhendeid, soovitusi ja dokumentide näidiseid, nii paberkujul kui ka veebis.

Oluline on toimepidevuse alaste teadmiste jagamine – ettevõttesiseselt, läbi korraldavate asutuste, teenuseosutajate vahel valdkondlike kriisikoosolekute raames.

Toimepidevuse alase teadlikkuse tõstmisega on seotud ka järgnevad ettepanekud 7, 8 ja 9.

2. Panna paika strateegiline ajakava elutähtsate teenuste täpsustamiseks.

Intervjuudest on ilmnenud, et hetkel ei eksisteeri selget klassifitseerimist ja raske on määratleda, millised asutuse või ettevõtte alamteenused on elutähtsad. Äriliste eesmärkidega ettevõtete puhul kehtib enamasti seos, et paremini tagatakse nende süsteemide toimepidevust, mis on kasumlikumad ja nii võib potentsiaalselt tekkida olukord, kus kriitilisema süsteemi kaitseks panustatakse vähem ressursse. Praegune olukord, kus elutähtsad teenused ei ole üheselt määratud, tekitab segadust nii teenuseosutajate kui järelvalvet teostavate asutuste seas.

Samuti tuleks tähelepanu pöörata teatud teenustele, mida ei peeta veel elutähtsateks. Siinkohal saab näitena tuua digiretsepti süsteemi. Intsidendi analüüsist selgus, et süsteemi pikaajaline maasolek tekitas olukorra, kus saadud digiretsepti ei olnud võimalik lunastada haigete väikelaste hooldajatel ja vähihaigetel, kelle jaoks on kriitiline õigeaegne valuvaigistite manustamine. Tegemist on teenusega, mille katkemine ohustab otseselt inimese elu ja tervist ning seetõttu liigitub see selgelt elutähtsa teenuse definitsiooni alla. Samuti võiks elutähtsate teenuste alla kuuluda ka ID-kaardi toimimine, täpsemalt

sertifitseerimisteenuse toimimine. Viimane on aluseks pangatoimingute tegemisel, samuti takistavad võimalikud häired digiallkirja andmist ja selle kehtivuse kontrollimist.

3. **Tõsta elutähtsate teenuste infosüsteemide ja –varade turvameetmete rakendamise prioriteeti.**

Meetmete väljatöötamine on pikaajaline protsess, samuti võtab määruse jõustumine aega. Intervjuudest on selgunud, et ühegi uue määruse rakendamine ei õnnestu kohe, tuleb leida vajalikud ressursid ja kompetents, et protsessi alustada ja edukalt lõpule viia. ISKE rakendamise ja toimepidevusplaanide koostamise pealt on näha, et taolised tegevused võivad võtta aastaid. Kõik arengusuunad näitavad infotehnoloogilise sõltuvuse suurt kasvu lähiaastatel ning selleks tuleb olla toimepidevuse alaselt valmis – omada juba teatud praktilist kogemust turvameetmete rakendamisel.

4. **Paika panna virtuaalse situatsiooniruumi strateegiline arengukava ja lahendada lahtised küsimused.**

Virtuaalne situatsiooniruum on järgmine arengusamm elutähtsate teenuste monitooringus ja kriisijuhtimises. Selleks, et süsteem saaks seaduslikel alustel toimima hakata, tuleb üheselt kindlaks määrata kes on süsteemi omanik, mis on selle eesmärk ja millist infot hakatakse koguma.

Eelmises peatükis toodi välja ka süsteemiga seotud ärihuvide kaitsmise küsimus – juhid ei soovi konkurentsiga sensitiivset teavet jagada. Selle probleemi võiks osaliselt kuni täielikult lahendada Sharemind raamistiku kasutamine, mis on teadusuuringutel põhinev süsteem andmestike privaatsust säilitavaks töötlemiseks [80, 81].

5. **Luua intsidentide andmebaas.**

Hetkel puudub riiklikul tasandil korrastatud andmekogu intsidentide kohta. Andmebaasi kogunenud info põhjal oleks võimalik läbi viia statistilist analüüsi, et välja selgitada, millised on intsidentide põhipõhjused ning vastavalt sellele suunata ennetustööd. Intsidentide andmebaasi võiks käsitleda ka virtuaalse situatsiooniruumi ühe osana.

6. **Muuta riskianalüüsi metoodikat.**

Intervjuudest on selgunud, et praegune riskianalüüsi läbi viimise metoodika on keeruline ja etteantud riskid ei pruugi kõiki reaalseid riske ära katta. Elutähtsate teenuste osutajad on

väga erinevad, seetõttu oleks vajalik valdkondlikult riske spetsiifilisemalt eristada. Siinkohal võib abiks tulla intervjuudes välja käidud ohukaardi idee.

7. Tõhustada elutähtsate teenuste järelvalvet.

Toimepidevuse tagamine seadusandlikus võtmes on uus temaatika ja kõigi osapoolte rollid ei ole veel praktilisel tasemel selged. Eriti keeruline olukord on omavalitsustes, kus ei ole koordineerimise jaoks piisavalt spetsialiste. Siiamaani on jäänud arusaamatuks, millistel alustel tuleks järelvalvet teostada. Korraldavates asutustes on vaja läbi viia koolitused, mis selgitavad esitatud analüüside ja plaanide kontrollimise metoodikat. Tuleb välja tuua, kuidas kontrollida juhendile vastavust ja millistele osadele rohkem tähelepanu pöörata. Kui järelevalve teostajad oskavad plaane analüüsida ja puudusi märgata, saavad nad teha ka parandusettepanekuid ja elutähtsate teenuste osutajaid dokumentide koostamisel aidata sellisel kujul nagu seadus seda praegu ette näeb.

Hetkel on omavalitsustes terav inimressursipuudus ja toimepidevusplaanidega tegelevad piiratud arv ametnikke oma põhitöökohustuste kõrvalt. See süvendab olukorda, kus omavalitsus funktsioneerib pigem edastava toruna teenuseosutajate ja Siseministeeriumi vahel ja plaanide kontroll on olematu või väga pinnapealne. Siinkohal oleks vaja kirjutada toimepidevuse koordineerimisega seotud tegevused ametikirjeldustesse või siiski leida ressursid konkreetselt toimepidevusega tegeleva spetsialisti palkamiseks.

8. Jätkata ISKE-alaste koolitustega ja viia läbi rohkem koolitusi elutähtsate teenuste osutajatele.

Intervjuudest on selgunud, et elutähtsa teenuse osutajaid on koolitatud väga vähe. Toimepidevuse riskianalüüsi ja toimepidevusplaani koostamise juhendid on keerulised ning need on vaja lahti seletada. Tähtis on selgitada toimepidevuse tagamise vajaduse olemust ja juhtida tähelepanu ennetustööle. Samuti on oluline õpetada tähelepanu pöörama seostele ja sõltuvustele põhi- ja tugiprotsesside vahel.

9. Hakata läbi viima simulatsiooniharjutusi ISKE rakendajatele ja elutähtsate teenuste osutajatele.

Intervjuudest on selgunud, et mitmed asutused ja ettevõtted ei vii läbi harjutusi ega testi olemasolevate toimepidevusplaanide töökindlust. Paljudel juhtudel ei olegi võimalik süsteeme tervikuna operatiivselt testida. Selle juures on abi peatükis 2.8 kirjeldatud

simulatsioonitestidest, mida on võimalik läbi viia oluliselt väiksema ressursikuluga. Simulatsiooniharjutuste tegemist saab käsitleda intensiivkoolitusena, millel on mitu positiivset mõju – sama valdkonna esindajad saavad kõikvõimalikud erinevad ohustsenaariumid paberil läbi mängida ning hiljem tagasisidefaasis omavahel kogemusi jagada ja tulemusi hinnata.

KOKKUVÕTE

Antud magistritöö andis ülevaate toimepidevuse tagamise teooriast ja korraldusest avalike teenuste osutamisel Eestis.

Esmalt tutvustati toimepidevuse tausta ja lähiaastate arenguid Eestis ja mujal maailmas. Töö teoreetilises osas kirjutati süstemaatiliselt lahti toimepidevuse tagamise protsessi tegevused ja muud seotud asjaolud.

Praktilises osas viidi läbi intervjuud ISKE-ga reguleeritud ja hädaolukorra seaduse alusel opereerivate avalike teenuste valdkondade esindajatega. Saadud informatsiooni põhjal koostati ülevaated teenuste toimepidevuse olukorrast. Samuti uuriti viimastel aastatel enim meediakajastust saanud intsidente ja esitati neist kompaktsed juhtumikirjeldused.

Kogutud informatsiooni analüüsimisel selgus, et üldine teenuste toimepidevuse olukord on hea – ükski teenus ei ole häiritud olnud rohkem kui paar ööpäeva, samuti ei ole viimastel aastatel tekkinud ühtegi väga suure mõjuga kriisiolukorda. Paraku ei saa kuidagi otsustada, kas tegemist on eduka riskide maandamisega või lihtsalt õnneliku juhusega. Valdkonna süvendatud uurimisel selgus, et toimepidevuse tagamisel on palju arenguruumi ja mitmed väljakutsed ootavad lahendust. Alahinnatakse sõltuvust infotehnoloogilistest vahenditest, mis suureneb tõenäoliselt lähiaastatel veelgi.

Saadud teadmiste põhjal identifitseeriti olulisemad kitsaskohad ning antud magistritöö autor esitas üheksa ettepanekut toimepidevuse tagamise edendamiseks.

Üks magistritöö eesmärkidest oli toimepidevuse alase teadlikkuse tõstmine. Töö autor on saanud juba intervjueeritavatelt positiivset tagasisidet, et läbiviidud vestlused panid rohkem mõtlema toimepidevuse tagamise aspektidele ja tuletasid meelde, et teatud toimepidevusega seotud tegevused on üldise töökorralduse seas märkamatult tagaplaanile jäänud.

Antud magistritöö võib tulevikus olla sisendiks:

1. Toimepidevuse alasele loengule või loengukursusele
2. Toimepidevuse alasele artiklile
3. Toimepidevuse tagamist tutvustavale juhendmaterjalile

Antud töö keskendus avalike teenuste toimepidevuse korralduse hindamisele, kuna erasektori ettevõtete turvalisuse olukorrast puudub üldine statistika ja avalikult oma meetmetest rääkida ei soovita. See on hästi mõistetav, kuna turvalisuse olukorra avaldamine on juba iseenesest turvarisk. Erasektori olukorra kaardistamine ja edendamine on järgmine oluline väljakutse. Seda eriti tänapäevases majandussituatsioonis, kus olemasolevate ja loodavate ettevõtete püsimine ja areng on ühiskondlikust seisukohast äärmiselt suure tähtsusega.

BUSINESS CONTINUITY MANAGEMENT AND OVERVIEW OF ITS IMPLEMENTATION IN PUBLIC SERVICES OF ESTONIA

Master's Thesis

Eveli Pung

SUMMARY

The main purpose of this thesis is to raise awareness regarding business continuity management. Two major goals are providing clear and concise guidelines in Estonian language for implementing business continuity measures and giving an overview of its progress in public services of Estonia.

This thesis begins with giving a general background of business continuity management in Estonia as well as other countries. A short overview of history, trends, statistics, standards, federal regulations and implementation guides is provided. It is followed by a detailed breakdown of actions needed to implement business continuity management. This theoretical part introduces conducting business impact analysis and risk analysis, managing risks, compiling business continuity plans, considering budgets, staffing teams and dealing with crisis communication.

The second part of this thesis focuses on public services in Estonia. Different interviews were carried out with representatives of various public services, including life-critical services, ministries and local governments who coordinate them and officials who regulate business continuity management on a federal level. The conducted interviews enabled compiling overviews of the different aspects of implementing business continuity in public services.

Gathered information showed that public services have not been affected by extensive crisis in the last years. None of the life-critical services have been disrupted for more than a few days. It remains unknown if that is an indication of good risk management or simply good fortune. However, by looking into business continuity measures more thoroughly, it became apparent that there is room for improvement and some challenges still need solutions. Based on the information gathered from those interviews, governmental analysis

documents and media, the author proposed nine suggestions to improve business continuity management.

The author of this thesis has already received positive feedback that the interviews carried out raised participants' awareness and reminded them to prioritize implementing continuity measures.

VIITED

[1] Hädaolukorra seadus. RT I, 30.12.2011, 44.

https://www.riigiteataja.ee/akt/13320720 (viimati vaadatud 01.01.2012)

[2] Paul Kirvan. Business Continuity: Business Continuity, A History of Challenges. Survival Instincts, 2007.

http://survivalinsights.com/modules.php?name=News&file=article&sid=6

(viimati vaadatud 01.01.2012)

[3] Disaster planning and business continuity after 9/11. ComputerWeekly.com, 2007.

http://www.computerweekly.com/Articles/2007/09/07/226632/Disaster-planning-and-business-continuity-after-911.htm (viimati vaadatud 01.01.2012)

[4] Siseministeeriumi kodulehekülg. Elutähtsad valdkonnad ja teenused.

http://www.siseministeerium.ee/elutahtsad-valdkonnad-ja-teenused-2/

(viimati vaadatud 01.01.2012)

[5] Wikipedia. 2008 submarine cable disruption.

http://en.wikipedia.org/wiki/2008_submarine_cable_disruption

(viimati vaadatud 01.01.2012)

[6] Wikipedia. Stuxnet.

http://en.wikipedia.org/wiki/Stuxnet (viimati vaadatud 01.01.2012)

[7] Toomas Kirt, Jaak Tepandi. Aasta 2000 on probleem ka Eestis. IT haldusjuhtimises, aastaraamat 1998.

http://www.riso.ee/et/pub/1998it/15.htm (viimati vaadatud 01.01.2012)

[8] Finantsinspektsiooni 2004. aasta aastaaruanne.

http://www.fi.ee/failid/FI2004.pdf (viimati vaadatud 01.01.2012)

[9] Välisministeeriumi koduleheküIg. Eesti virtuaalsel lahinguväljal. Teadlikud kodanikud ja K5 tagavad Eestile küberkaitse. Pilk peeglisse 2009.

http://www.vm.ee/?q=node/9058 (viimati vaadatud 01.01.2012)

[10] NATO Cooperative Cyber Defence Centre of Excellence koduleheküIg.

http://www.ccdcoe.org/ (viimati vaadatud 01.01.2012)

[11] Riigi Infosüsteemi Ameti koduleheküIg. ISKE. Korduma Kippuvad Küsimused.

http://www.ria.ee/28416 (viimati vaadatud 01.01.2012)

[12] Mel Gosling, Andrew Hiles. Business Continuity Statistics: Where Myth Meets Fact

http://www.continuitycentral.com/feature0660.html (viimati vaadatud 01.01.2012)

[13] Trouble Shooters Technical Support. Disaster Recovery and Business Continuity Planning.

http://www.troubleshootersts.com/it-solutions/disaster-recovery-and-business-continuity-planning.aspx (viimati vaadatud 01.01.2012)

[14] AllTek Services koduleheküIg.

http://alltekservices.com/it_solutions/disaster_recovery_and_business_continuity_planning.html (viimati vaadatud 01.01.2012)

[15] Leap Technologies koduleheküIg.

http://www.leaptechnologies.ca/Professional%20Services.html

(viimati vaadatud 01.01.2012)

[16] Arces Network koduleheküIg.

http://arces.net/solutions/business/bdr-for-business/ (viimati vaadatud 01.01.2012)

[17] cyberMIND Corporation koduleheküIg.

http://www.cybermind-usa.com/disaster-recovery-and-continuity-planning.html

(viimati vaadatud 01.01.2012)

[18] CG Tech Services koduleheküg.

http://www.cgtechservices.com/services.html (viimati vaadatud 01.01.2012)

[19] Eesti Statistika. Arvuteid kasutavad ettevõtted tegevusala (EMTAK 2008) ja tööga hõivatud isikute arvu järgi.

http://pub.stat.ee/px-web.2001/Database/Majandus/05Infotehnoloogia/02Infotehnoloogia_ettevettes/02Infotehnoloogia_ettevettes.asp (viimati vaadatud 01.01.2012)

[20] Wikipedia. Business continuity planning.

http://en.wikipedia.org/wiki/Business_continuity_planning

(viimati vaadatud 01.01.2012)

[21] BSI standard 100-4. Hädaolukordade haldus. 2008

http://www.ria.ee/public/ISKE/BSI_standard_1004.pdf (viimati vaadatud 01.01.2012)

[22] Marianne Swanson, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, David Lynes. Contingency Planning Guide For Federal Information Systems. Nist Special Publication 800-34 Rev.1.

http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf (viimati vaadatud 01.01.2012)

[23] Toimepidevuse plaani koostamise juhend. RT I 2010, 33, 180

https://www.riigiteataja.ee/akt/13326401 (viimati vaadatud 01.01.2012)

[24] Finantsinspektsiooni soovituslik juhend. Nõuded finantsjärelevalve subjekti talitluspidevuse protsessi korraldamisele. Finantsinspektsioon, 2009.

http://www.fi.ee/failid/Juhend_20091104_Talitluspidevus.pdf

(viimati vaadatud 01.01 2012)

[25] IT-turbejuhend. Lühiülevaade olulisematest IT-turbe alastest turvameetmetest. Riigi Infosüsteemi Amet, 2009.

http://ria.ee/public/ISKE/Infoturbe_soovituste_juhend_v1.pdf

(viimati vaadatud 01.01.2012)

[26] Paul H. Rosenthal in collaboration with L. Jane Park and Jan I. Weissman. Business Continuity Management: A Tutorial with Case Studies, California State University, Los Angeles, 2008.

http://instructional1.calstatela.edu/prosent/Business%20Continuity%20Management-%20a%20tutorial%20with%20Case%20Studies.pdf (viimati vaadatud 01.01.2012)

[27] Erkki Leego. Andmeturbe teooria ja praktika tasakaal. 2010.

http://www.hlp.ee/Ettekanded/Andmeturbe_teooria_ja_praktika_tasakaal_10_06_2010_Leego.pdf (viimati vaadatud 01.01.2012)

[28] Toimepidevuse riskianalüüsi koostamise juhend. RT I 2010, 33, 179.

https://www.riigiteataja.ee/akt/13326405 (viimati vaadatud 01.01.2012)

[29] Infosüsteemide kolmeastmelise etalonturbe süsteem ISKE kataloogid. ISKE rakendusjuhendi Lisa 1. Versioon 5.00, 2009.

http://ria.ee/public/ISKE/iske_kataloogid_5_00.pdf (viimati vaadatud 01.01.2012)

[30] Martin Hanson. Suurim kindlustuskahju seni on Pärnu üleujutus. Äripäev, 2007.

http://www.ap3.ee/default.aspx?PublicationId=31503ED6-39D4-4163-9D98-74AA1E3959CE&code=3756/uud_uudidx_375601 (viimati vaadatud 01.01.2012)

[31] Inno Tähismaa, Andras Kralla. Üleujutusest räsitud Pärnu kiirustab taas uksi avama. Äripäev, 2005.

http://www.ap3.ee/?PublicationId=31503ED6-39D4-4163-9D98-74AA1E3959CE&code=2787/uud_uudidx_278705 (viimati vaadatud 01.01.2012)

[32] Mark S. Dorfman. Introduction to Risk Management and Insurance (9 ed.). Englewood Cliffs, N.J: Prentice Hall, 2007.

[33] Hansson, Leego & Partner OÜ kodulehekülg. Talitluspidevuse planeerimine.

http://www.hlp.ee/Kuidas_teeme3b.htm (viimati vaadatud 01.01.2012)

[34] ConsultIT OÜ kodulehekülg. Talitluspidevus.

http://consultit.ee/?id=63 (viimati vaadatud 01.01.2012)

[35] KPMG Baltics OÜ kodulehekülg. Talitluspidevuse planeerimine.

http://www.kpmg.com/EE/et/WhatWeDo/Noustamine/Juhtimisnoustamine/Infosysteemid/Lehed/Talitluspidevuse-planeerimine.aspx (viimati vaadatud 01.01.2012)

[36] Kristjan Akkermann. Talitluspidevusplaan – mida teha, kui 1.jaanuaril esinevad probleemid. 2010.

http://www.asaquality.ee/images/euro2010/4_Talitluspidevus_Kristjan_Akkermann.pdf

(viimati vaadatud 01.01.2012)

[37] Carl M. Evans. BCP Awareness Training. 2004.

http://capitaloftexas.acp-international.com/publications/BCP%20Training%20Program%20Overview.ppt

(viimati vaadatud 01.01.2012)

[38] Kaja Tampere. Ausus säilitab usaldust. Äripäev, 2003.

http://www.ap3.ee/?PublicationId=31503ED6-39D4-4163-9D98-74AA1E3959CE&code=2339/rubr_turundus (viimati vaadatud 01.01.2012)

[39] Valitsuskommunikatsiooni käsiraamat. Riigikantselei, 2010.

http://www.valitsus.ee/UserFiles/valitsus/et/uudised/valitsuskommunikatsioon/valitsuskommunikatsiooni_kasiraamat_2010.pdf (viimati vaadatud 01.01.2012)

[40] Richard Cyert and James March. Behavioral Theory of the Firm. Oxford: Blackwell, 1963.

[41] Margus Kreinin. Avalikud teenused – kuidas luau kodanikule meelepäraseid ja omavahel integreeritud teenuseid?

http://dw.riik.ee/@api/deki/files/92/=SiM-Avalike_teenuste_ettekanne13_03.pptx

(viimati vaadatud 01.01.2012)

[42] Riigi Infosüsteemi Ameti kodulehekülg. ISKE.

http://www.ria.ee/iske (viimati vaadatud 01.01.2012)

[43] Infosüsteemide turvameetmete süsteem. RT I 2007, 71, 440

https://www.riigiteataja.ee/akt/13125331 (viimati vaadatud 01.01.2012)

[44] Avaliku teabe seadus. RT I, 22.03.2011, 9.

https://www.riigiteataja.ee/akt/122032011009 (viimati vaadatud 01.01.2012)

[45] Infosüsteemide andmevahetuskiht. RT I 2008, 18, 129.

https://www.riigiteataja.ee/akt/12956835 (viimati vaadatud 01.01.2012)

[46] ISKE rakendamise alane küsitlus. Riigi Infosüsteemi Amet, 2010.

http://ria.ee/public/ISKE/ISKE_rakendamise_alane_k_sitlus_tulemused_mai_2010.pdf

(viimati vaadatud 01.01.2012)

[47] Riigi Infosüsteemi Ameti kodulehekülg. Järelvalve osakond.

http://ria.ee/jarelevalve-osakond (viimati vaadatud 01.01.2012)

[48] 2011.aasta hädaolukordade riskianalüüside kokkuvõte. Siseministeerium, 2011.

http://www.siseministeerium.ee/public/HO_RA_2011.pdf (viimati vaadatud 01.01.2012)

[49] Eesti Haigekassa kodulehekülg. Digiretsept.

http://www.haigekassa.ee/digiretsept (viimati vaadatud 01.01.2012)

[50] Evelin Koppel. 1. jaanuarist 2010 hakkab kehtima digiretsept. Haigekassa kodulehekülg, 2009.

http://www.haigekassa.ee/haigekassa/uudised?news=1-jaanuarist-2010-hakkab-keht

(viimati vaadatud 01.01.2012)

[51] Marina Lohk. Danilov: digiretsepti seiskas viga andmebaasis. Tarbija24, 2010.

http://www.tarbija24.ee/211424/danilov-digiretseptisusteemi-seiskas-viga-andmebaasis/

(viimati vaadatud 01.01.2012)

[52] Eger Ninn. Ravimite soodustused tekitavad digiretsepti süsteemis segadust. Tarbija24, 2010.

http://www.tarbija24.ee/207973/ravimite-soodustused-tekitavad-digiretsepti-susteemis-segadust/ (viimati vaadatud 01.01.2012)

[53] Marina Lohk. Digiretseptikesuse rike jättis osa inimesi ravimita. Tarbija24, 2010.

http://www.tarbija24.ee/211349/digiretseptikeskuse-rike-jattis-osa-inimesi-ravimita/

(viimati vaadatud 01.01. 2012)

[54] Siiri Erala. Digiretsept tõrkus taas. Tarbija24, 2010.

http://www.tarbija24.ee/215239/digiretsept-torkus-taas/ (viimati vaadatud 01.01.2012)

[55] Siiri Erala. Digiretsepti süsteemis oli taas rike. Tarbija24, 2010.

http://www.tarbija24.ee/219993/digiretsepti-susteemis-oli-taas-rike/

(viimati vaadatud 01.01.2012)

[56] Ester Vilgats. Ülekoormus põhjustas taas tõrkeid digiretseptide töös. ERR, 2010.

http://uudised.err.ee/index.php?06196609 (viimati vaadatud 01.01.2012)

[57] Sven Randlaid. Ministeerium: digiretseptisüsteem on sügiseks töökindel. ERR, 2010.

http://uudised.err.ee/index.php?06200418 (viimati vaadatud 01.01.2012)

[58] Kadri Ratt. Digiretseptide väljastamine oli mitu tundi häiritud. Tarbija24, 2010.

http://www.tarbija24.ee/340884/digiretseptide-valjastamine-oli-mitu-tundi-hairitud/

(viimati vaadatud 01.01.2012)

[59] Sirje Niitra. Digiretsept streikis jälle. Tarbija24, 2011.

http://www.tarbija24.ee/404851/digiretsept-streikis-jalle/ (viimati vaadatud 01.01.2012)

[60] Katrin Jürisoo. Ansip: digiretsept on suur pettumus. ERR, 2010.

http://uudised.err.ee/index.php?06200489 (viimati vaadatud 01.01.2012)

[61] Marina Lohk. Haigekassa: tõrge tekkis täis saanud tabeli tõttu. Tarbija24, 2010.

http://www.tarbija24.ee/211962/haigekassa-torge-tekkis-tais-saanud-tabeli-tottu/

(viimati vaadatud 01.01.2012)

[62] Karin Koppel. Tulemuste kuvamist segas andmebaasimootori viga. ERR, 2011.

http://uudised.err.ee/index.php?06225197 (viimati vaadatud 01.01.2012)

[63] Vabariigi Valimiskomisjoni infosüsteemi avaliku liidese tehniline audit. Asa Quality Services, 2011.

http://www.vvk.ee/public/ASA_raport.pdf (viimati vaadatud 01.01.2012)

[64] Sven Randlaid. Sibul: katkestus pani valimiste usaldusväärsuse löögi alla. ERR, 2011.

http://uudised.err.ee/index.php?06225201 (viimati vaadatud 01.01.2012)

[65] Katrin Jüriso. Eksperdid ei usu Helmese eneseõigustusi. ERR, 2011.

http://uudised.err.ee/index.php?06225391 (viimati vaadatud 01.01.2012)

[66] Vabariigi Valimiskomisjoni kiri Helmes AS esindajale. 08.04.2011.

http://www.riigikogu.ee/?op=emsplain&page=pub_pub_dynobj_file&pid=1330710&file_id=1330727&content_type=application/pdf&file_name=20110804579-1.pdf&file_size=104325&wdtid=180403&u=20110531013827

(viimati vaadatud 01.01.2012)

[67] Elektrinäidu teatamisel võib esineda häireid. Eesti Energia kodulehekülg, 2011.

https://www.energia.ee/et/about/presscentre/news/press (viimati vaadatud 01.01.2012)

[68] Eesti Energia infosüsteem võttis mai esimesel nädalal vastu üle poole miljoni näidu. Eesti Energia kodulehekülg. 2011.

https://www.energia.ee/et/about/presscentre/news/press (viimati vaadatud 01.01.2012)

[69] Siiri Erala. Elektrinäidu teatamine on takistatud. Tarbija24, 2011.

http://www.tarbija24.ee/428109/elektrinaidu-teatamine-on-takistatud/

(viimati vaadatud 01.01.2012)

[70] Siiri Erala. Eesti Energia kliendiinfosüsteem takistas taas elektrinäidu teatamist. Tarbija24, 2011.

http://www.tarbija24.ee/454534/eesti-energia-kliendiinfosusteem-takistas-taas-elektrinaidu-teatamist/ (viimati vaadatud 01.01.2012)

[71] Raigo Neudorf. Elioni internetiüendus oli üle eesti häiritud. E24, 2011.

http://www.e24.ee/343119/elioni-internetiuhendus-oli-ule-eesti-hairitud/

(viimati vaadatud 01.01.2012)

[72] Kadrin Karner. Elion: tuumikvõrgu rike oli erakordne juhtum. Äripäev, 2010.

http://www.ap3.ee/?PublicationId=c07edbce-c534-459d-9349-152fcd3eaee7

(viimati vaadatud 01.01.2012)

[73] Raigo Neudorf. Elion: tegu oli erakordse juhtumiga. E24, 2010.

http://www.e24.ee/343358/elion-tegu-oli-erakordse-juhtumiga/

(viimati vaadatud 01.01.2012)

[74] Raigo Neudorf. EMT võrgurikke tõttu oli häiritud 750 000 kliendi mobiilside. E24, 2010.

http://www.e24.ee/350958/emt-vorgurikke-tottu-oli-hairitud-750-000-kliendi-mobiilside/

(viimati vaadatud 01.01.2012)

[75] Raigo Neudorf. Elioni tehniline rike põhjustas terves Eestis palju segadust. E24, 2010.

http://www.e24.ee/343694/elioni-tehniline-rike-pohjustas-terves-eestis-palju-segadust/

(viimati vaadatud 01.01.2012)

[76] Raigo Neudorf. Inimesed ei saanud helistada hädaabinumbrile 112. E24, 2010.

http://www.e24.ee/343206/inimesed-ei-saanud-helistada-hadaabinumbrile-112/

(viimati vaadatud 01.01.2012)

[77] Raigo Neudorf. Elion suurendab rikke tõttu investeeringuid tuumikvõrku. E24, 2010.

http://www.e24.ee/344660/elion-suurendab-rikke-tottu-investeeringuid-tuumikvorku/

(viimati vaadatud 01.01.2012)

[78] Raigo Neudorf. EMT tuumikvõrgu rikke põhjustas ruuteri riistvara. E24, 2010.

http://www.e24.ee/351691/emt-tuumikvorgu-rikke-pohjustas-ruuteri-riistvara/

(viimati vaadatud 01.01.2012)

[79] Riigi Infosüsteemi Ameti koduleheküg. Tark e-riik.

http://www.ria.ee/tark-e-riik-2011 (viimati vaadatud 01.01.2012)

[80] Dan Bogdanov, Riivo Talviste, Jan Willemson. Deploying secure multi-party computation for financial data analysis. University of Tartu, Institute of Computer Science, 2011.

http://eprint.iacr.org/2011/662.pdf (viimati vaadatud 01.01.2011)

[81] Sharemind projekti kirjeldus.

http://dan.bmonde.net/koduleht/Projektid/94FF4AEF-A1D9-4AD3-B3AF-F9976571A01B.html (viimati vaadatud 01.01.2011)

LISAD

LISA 1. INTERVJUUKÜSIMUSED ISKE KORRALDAJALE RIIKLIKUL TASEMEL

1. Milline on Teie ja asutuse roll ISKE korraldamisel?
2. Kui palju on riiklikke andmekogusid, millele rakendatakse ISKE-t?
3. Kui paljud asutused on ISKE-t rakendanud?
4. Kui paljudes asutustes on ISKE rakendamist auditeeritud?
5. Kuidas hindate ISKE rakendamise kvaliteeti?
6. Millist analüüsi on läbi viidud ISKE auditeerimise tulemuste pealt?
7. Millised asutused on ISKE rakendamisel edukamad ja millised vähemedukamad?
8. Millist kompetentsi kasutatakse ISKE rakendamisel? Kas rakendatakse omapäi, palutakse abi või ostetakse vastavat teenust sisse?
9. Kui oluliseks peetakse ISKE rakendamisel käideldavuse aspekti?
10. Kui palju on riiklikke andmekogusid, mille käideldavuse turvaosaklass on kõige kõrgem (K3) ?
11. Milliseid suuremaid katkestusi on viimastel aastatel esinenud?
12. Millised asjaolud kõige tihedamini intsidente põhjustavad?
13. Millisel viisil peate arvet intsidentide üle?
14. Kuidas toimib intsidentidest teavitamine?
15. Kuidas tagatakse elutähtsate teenuste osutajate infosüsteemide toimepidevus?
16. Milliseid ISKE koolitusi on läbi viidud?
17. Millised on koolitustega seotud väljakutsed?
18. Milliste väljakutsetega tuleb veel tegeleda ISKE valdkonnas?

19. Millised on järgmiste aastate arenguplaanid ISKE vallas?

20. Milliseid materjale leidub ISKE rakendamise kohta?

LISA 2. INTERVJUUKÜSIMUSED ISKE RAKENDAJALE

1. Milline on Teie roll asutuse toimepidevuse korraldamisel?
2. Kui palju on teie asutusel infosüsteeme?
3. Millised neist on kõige kriitilisemad?
4. Kas infosüsteemidele on ISKE rakendatud?
5. Kes tegeleb ISKE rakendamisega?
6. Kas infosüsteemidele on toimepidevusplaanid olemas?
7. Millisel viisil peate arvet intsidentide üle?
8. Kas intsidentide kohta tehakse ka statistilist analüüsi?
9. Milliseid suuremaid intsidente on viimastel aastatel juhtunud?
10. Millisel viisil on tagatud infosüsteemide toimepidevus?
11. Kui suur on infosüsteemide tähtsus igapäevatöös?
12. Kui pikaks ajaks võib töö seiskuda enne kui sellega kaasnevad rängad tagajärjed?
13. Kuidas muutub Teie hinnangul sõltuvus IT-st järgmiste aastate jooksul?
14. Millised väljakutsed on praegu seoses infosüsteemide haldamisega?
15. Kui palju eraldatakse üldeelarvest IT valdkonnale? Kui palju sellest toimepidevusele?
16. Kas tippjuhtkond mõistab IT investeeringute vajadust?
17. Kas asutuses on määratud infoturbejuht?
18. Millised on tulevikuplaanid infosüsteemide osas?
19. Millised on infosüsteemide käideldavuse eesmärgid?
20. Mida ootate riigilt seoses ISKE koordineerimisega?
21. Milliseid materjale leidub ISKE rakendamise kohta teie asutuses?

LISA 3. INTERVJUUKÜSIMUSED TOIMEPIDEVUSE ALASE SEADUSANDLUSE KOOSTAJALE

1. Milline on Teie ja asutuse roll toimepidevuse tagamisel?
2. Mis on elutähtis teenus?
3. Kas elutähtsate teenuste osutajad mõistavad toimepidevuse olemust ja vajadust?
4. Millist tagasisidet olete saanud toimepidevuse tagamise kohta?
5. Millised elutähtsate teenuste osutajad on valdkonniti edukamad ja millised vähemedukamad?
6. Kui palju on tehtud toimepidevusalaseid koolitusi?
7. Kuidas toimib plaanide esitamise ahel?
8. Mida näitas koostatud koondülevaade?
9. Milliseid suuremaid intsidente on viimastel aastatel ette tulnud?
10. Millisel viisil peate arvet intsidentide üle?
11. Millisel viisil on koondülevaates kajastatud IT-sõltuvus?
12. Kuidas muutub Teie hinnangul sõltuvus IT-st järgmiste aastate jooksul?
13. Kuidas on plaanis IT osa seadusega reguleerida?
14. Kuidas hindate praegust juhendmaterjali toimepidevuse riskianalüüsi ja toimepidevusplaani koostamiseks?
15. Kuidas peaksid elutähtsa teenuse toimepidevust korraldavad asutused kontrollima esitatud toimepidevuse riskianalüüsi ja toimepidevusplaani kvaliteeti?
16. Kuidas kaardistatakse omavahelisi sõltuvusi valdkondade ja teenuste vahel?
17. Kuidas tagatakse valdkondlikku toimepidevust?
18. Mida näitas hädaolukorra seaduse analüüs?
19. Millised toimepidevust reguleerivad seadused on mujal Euroopas ja maailmas?

20. Milline on hädaolukorra seaduse strateegiline ajakava?
21. Kes on aktiivsed hädaolukorra seaduse väljatöötamisel?
22. Millised on Siseministeeriumi ootused elutähtsate teenuste osutajatele ja elutähtsate teenuste toimepidevust korraldavatele asutustele?
23. Milliseid materjale leidub elutähtsate teenuste osutajate toimepidevuse korralduse kohta?

LISA 4. INTERVJUUKÜSIMUSED IT-ALAST TOIMEPIDEVUST KORRALDAVALE ASUTUSELE

1. Milline on Teie ja asutuse roll elutähtsate teenuste toimepidevuse koordineerimisel?
2. Kui suur on hinnanguliselt IT-sõltuvus avalike teenuste osutamisel?
3. Mis on elutähtis teenus?
4. Milliste kriteeriumite alusel määratakse elutähtsate teenuste osutajaks?
5. Kuidas hindate toimepidevuse tagamise kvaliteeti?
6. Kas toimepidevuse riskianalüüs ja toimepidevusplaanid koostatakse omal käel või ostetakse kompetentsi sisse?
7. Kas seadusega sätestatud juhendmaterjal on piisav?
8. Millised on veel toimepidevusplaanidega seotud väljakutsed?
9. Kui palju testitakse toimepidevusplaane?
10. Kuidas on elutähtsate teenuste osutajate toimepidevuse tagamise olukord võrreldes ülejäänute avalike teenuste osutamisega?
11. Kuidas hindate ISKE rakendamise edukust?
12. Millised on teiste riikide arengud ja kuhu positsioneerub Eesti?
13. Kas toimepidevuse tagamine areneb samas tempos uute teenuste arenguga Eesti kui e-Riigi kontekstis?
14. Millisel viisil peetakse arvet intsidentide üle?
15. Kuidas jagunevad intsidendid raskusastmete järgi?
16. Kui palju on viimastel aastatel olnud intsidente?
17. Millistele riskidele pööratakse tänapäeval kõige rohkem tähelepanu?
18. Millistele riskidele pööratakse tänapäeval kõige vähem tähelepanu?
19. Millised on kõige tüüpilisemad katkestused?

20. Kui palju IT-eelarvest määratakse toimepidevuse tagamisele?

21. Mis on Virtuaalne situatsiooniruum?

22. Millal Virtuaalne situatsiooniruum tööle hakkab?

23. Kuidas valmistutakse küberrünnakuteks?

24. Kui palju viiakse läbi ISKE rakendamise ja toimepidevusealaseid koolitusi?

25. Millised väljakutsed ootavad lahendust elutähtsate teenuste toimepidevuse osas?

26. Millised on tulevikuplaanid elutähtsate teenuste toimepidevuse koordineerimisel?

27. Milliseid materjale leidub elutähtsate teenuste osutajate toimepidevuse kohta?

LISA 5. INTERVJUUKÜSIMUSED ELUTÄHTSA TEENUSE TOIMEPIDEVUST KORRALDAVALE ASUTUSELE

1. Milline on Teie ja asutuse roll elutähtsate teenuste osutajate toimepidevuse koordineerimisel?
2. Mitu erinevat elutähtsate teenuste osutajat on teie haldusalas?
3. Millised on väiksemad ja millised suuremad teenuseosutajad?
4. Kas elutähtsate teenuste osutajad on esitanud toimepidevusplaanid?
5. Millised elutähtsate teenuste osutajad on edukamad ja millised vähemedukamad?
6. Milline on esitatud toimepidevusplaanide kvaliteet?
7. Mille alusel hindate toimepidevusplaanide kvaliteeti?
8. Kas mõni elutähtsa teenuse osutaja on palunud teilt kui korraldavalt asutuselt abi toimepidevuse riskianalüüsi või toimepidevusplaani koostamisel?
9. Kas elutähtsate teenuste osutajad on aru saanud toimepidevuse olemusest ja vajadusest?
10. Kui palju viiakse läbi toimepidevusplaanide harjutusi?
11. Millisel viisil toimub intsidentidest teavitamine?
12. Millisel viisil peetakse arvet intsidentide üle?
13. Kas kogutud intsidentide põhjal tehakse ka analüüsi?
14. Milliseid suuremaid intsidente on viimastel aastatel juhtunud?
15. Milliseid intsidente on juhtunud elutähtsate teenuste osutajate IT-süsteemidega?
16. Kui palju kasutavad elutähtsate teenuste osutajad IT-d igapäevatöös?
17. Kuidas muutub Teie hinnangul sõltuvus IT-st järgmiste aastate jooksul?
18. Kuidas tagatakse valdkondlikku toimepidevust?

19. Kuidas hindate toimepidevuse riskianalüüsi ja toimepidevusplaani koostamise metoodikat?
20. Millised on veel väljakutsed seoses elutähtsate teenuste osutajate toimepidevuse koordineerimisega?
21. Millised on tulevikuplaanid elutähtsate teenuste toimepidevuse koordineerimisel?
22. Millised on teie ootused riigile seoses elutähtsate teenuste osutajate toimepidevuse koordineerimisega?
23. Milliseid materjale leidub elutähtsate teenuste osutajate toimepidevuse kohta?

LISA 6. INTERVJUUKÜSIMUSED ELUTÄHTSATE TEENUSTE OSUTAJATELE

1. Milline on Teie roll toimepidevuse koordineerimisel?
2. Millised on teie osutatavad elutähtsad teenused?
3. Milliseid infosüsteeme kasutate?
4. Mitu aastat olete tegelenud toimepidevuse tagamisega?
5. Millised on sisemised korrad, juhendid ja protseduurid?
6. Kas olete esitanud toimepidevuse riskianalüüsi ja toimepidevusplaani?
7. Kas olete saanud riskianalüüsile ja toimepidevusplaanile tagasisidet?
8. Kas olete protsessidele määranud nõutavad taastamisajad?
9. Kes koostab toimepidevusplaani? Kui suur on sisemine meeskond?
10. Kas seadusega sätestatud toimepidevuse riskianalüüsi ja toimepidevusplaani juhendmaterjal on piisav?
11. Kuidas hindate seaduses ära toodud riskianalüüsi läbiviimise metoodikat?
12. Kuidas suhtub tippjuhtkond toimepidevuse seisukohast vajalike muudatuste elluviimisesse?
13. Kuidas hindate üldiselt toimepidevuse tagamise olukorda?
14. Kui tihti korraldate toimepidevusplaani testimiseks harjutusi?
15. Mida on testid näidanud?
16. Kuidas olete taganud infosüsteemide toimepidevuse? (Generaatorid, varukoopiad jms)
17. Kas olete määranud kriisijuhi?
18. Kui palju on toimunud toimepidevusealaseid koolitusi?
19. Milliseid intsidente on viimaste aastate jooksul juhtunud?
20. Millisel viisil peate intsidentide üle arvet?

21. Kas kogutud intsidentide põhjal tehakse ka analüüsi?

22. Kuidas on korraldatud intsidentidest teavitamine?

23. Millised väljakutsed on veel seotud toimepidevuse tagamisega?

24. Kuidas muutub Teie hinnangul sõltuvus IT-st järgmiste aastate jooksul?

25. Millised on lähiaastate arenguplaanid toimepidevuse tagamisel?

26. Millised on teie ootused riigile seoses toimepidevuse tagamise koordineerimisega?

27. Milliseid materjale leidub asutuse toimepidevuse kohta?