TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Tarkvarateaduse instituut

Pavel Buzõkin 134564IABB

VÕRGUINTSIDENDI KAHTLUSE MENETLEMISE PROTSESSI ANALÜÜS

Bakalaureusetöö

Juhendaja: Karin Rava
MSc. Eng

Tallinn 2018

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Pavel Buzõkin

22.05.2018

Annotatsioon

Käesolevas bakalaureusetöös uuritakse infotehnoloogia ettevõtte võrguintsidendi kahtluse menetlemise protsessi. Töö eesmärgiks on analüüsida nimetatud äriprotsessi selle parendamise eesmärgil.

Töö esimeses pooles on antud ülevaade ettevõttes kasutusel olevatest protsessi raamistikest ning täpsemalt on uuritud teenuste opereerimise protsessi. Töö teises pooles analüüsitakse võrguintsidendi kahtluse menetlemise äriprotsessi, otsitakse selle kitsaskohti ning tuuakse välja parendusettepanekud.

Töö tulemusena on esitatud parendatud protsessi mudel ning pakutud välja idee uuest süsteemist, mille kaudu oleks võimalik võrguintsidendi kahtluseid menetleda. Uue süsteemi kohta on püstitatud nõuded ning dokumenteeritud vajalikud ärireeglid.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 27 leheküljel, 7 peatükki, 9 joonist.

Abstract

Analysis of Network Incident Suspicion Handling Process

The bachelor's thesis is about analysis of network incident suspicion handling process in an information technology company. The aim of the analysis it to find improvements in the process.

The first part of the thesis describes process frameworks which are used in the company, and Service Operations processes. In the second part of the thesis business process is analyzed to identify bottlenecks and bring out improvements.

As a result, a new network incident suspicion handling process has been modelled and a new system for handling network disturbance suspicions has been suggested. The requirements for the new system have been set and the business rules were listed.

The thesis is in Estonian and contains 27 pages of text, 7 chapters, 9 figures.

Lühendite ja mõistete sõnastik

AS IS	Äriprotsessi hetkeseisu kirjeldus
TO BE	Optimeeritud äriprotsess
SLA	*Service Level Agreement* Teenustase
eTOM	*Enhanced Telecom Operations Map*
ITIL	*Information Technology Infrastructure Library*
BPMN	Business Process Modeling Notation Äriprotsesside modelleerimiskeel
CRM	*Customer Relationship Management* Kliendisuhete juhtimine
KPI	*Key Performance Indicator* Tulemuslikkuse võtmemõõdik
Web API	*Web Application Programming Interface* Veebipõhine rakendusliides

Sisukord

Jooniste loetelu

1 Sissejuhatus

Bakalaureusetöö teemaks valis autor „Võrguintsidendi kahtluse menetlemise protsessi analüüs“. Autor valis selle teema, kuna on ise selle protsessiga kokku puutunud. Kokkupuute alusel leidis autor, et antud protsess ei ole töötajate jaoks kõige mugavam ning võrguintsidendi kahtluse menetlemise kiiruse ja kvaliteedi tagamine on keeruline.

1.1 Taust ja probleemi olemus

Bakalaureuse töö raames analüüsitakse võrguintsidendi kahtluse protsessi selle protsessi parendamise eesmärgil infotehnoloogia ettevõte näitel (edaspidi ettevõte). Antud protsess on olulise rolliga võrguintsidendi protsessi sees, olles üks selle protsessi sisendiks. Võrguintsidendi kahtlus annab võimaluse tuvastada sündmusi, mis ei ole kaetud monitooringuga ning mis ei tule välja alarmihalduse protsessi kaudu. Valdav enamus võrguintsidente tuvastatakse automaatse monitooringu kaudu. Võrguintsidendi kahtluste kaudu on võimalik tuvastada võrguintsidente jaotusvõrgus, TV sisus ning spetsiifilisemaid muresid rakenduste funktsionaalsuses. Võrguintsidendi kahtluse protsess täiendab sündmuste tuvastamise protsessi ning läbi selle tagatakse täielik sisend võrguintsidendi protsessile.

Hetkel toimub võrguintsidendi kahtluse menetlemine erinevates süsteemides, töötajad peavad käsitsi koostama e-kirja, kuhu sisse lisatakse või kopeeritakse informatsiooni püstitatud võrguintsidendi kahtluse kohta. Informatsioon võrguintsidentide ning võrguintsidendi kahtluste kohta asub erinevates kohtades.

1.2 Eesmärgid

Lõputöö eesmärkideks on:

1. Viia läbi võrguintsidendi kahtluse menetlemise protsessi analüüs selle parendamiseks
2. Dokumenteerida analüüsi tulemused ning ärireeglid

3. Tuua välja idee uue lahenduse kohta

1.3 Metoodika

Lõputöö eesmärkide saavutamiseks viib autor läbi vaatlused äriprotsessi analüüsimiseks ja intervjuud analüüsitava äriprotsessi tegutsejatega. Äriprotsessi kirjeldamiseks kasutatakse *Bizagi Process Management* [1] tarkvara ning *Business Process Modeling Notation* (BPMN) meetodit. BPMN on modelleerimiskeel, mille kasutamisel on võimalik äriprotsessi graafiliselt noteerida. Antud meetod on arusaadav nii IT kui ka äri osapooltele. [2]

Äriprotsessi põhitegutsejateks on töötajad Kasutajatoest, Seirekeskusest. Samuti küsis autor sisendit kvaliteedianalüütiku käest, kelle ülesandeks on teenuste opereerimise protsesside kvaliteedi aruandlus.

Uue süsteemi funktsionaalsuse kirjeldamisel kasutab autor protsessi tegutsejate käest saadud sisendit.

1.4 Ülevaade lõputööst

Bakalaureuse töö koosneb sissejuhatusest, 5 peatükist ning kokkuvõttest. Teine peatükk annab ülevaate ettevõtte protsessikesksest juhtimisest. Samuti on lühidalt kirjeldatud teenuste opereerimise protsesse.

Kolmandas peatükis analüüsib autor võrguintsidendi kahtluse menetlemise protsessi (AS IS). Analüüsi tulemused esitatakse graafiliselt ning seejärel kirjeldatakse. Lisaks tuuakse välja analüüsitud protsessi kitsaskohad ning parendusettepanekud.

Neljandas peatükis esitab autor optimeeritud (TO-BE) protsessi. Äriprotsess esitatakse graafiliselt ja sellele järgneb protsessi kirjeldus. Samuti kirjeldatakse ärireegleid ning võrguintsidendi kahtluse menetlemise kvaliteedi aruandlust.

Viiendas peatükis esitab autor idee uue süsteemi kohta, mis toetab optimeeritud äriprotsessi. Autor määratleb selle funktsionaalsed ja mittefunktsionaalsed nõuded, esitab uue süsteemi prototüübi ning tähtsamad liidestused teiste süsteemidega. Kuuendas peatükis esitab autor süsteemi kasutusjuhtude diagrammi, nende kirjeldused ning võrguintsidendi kahtluse olekudiagrammi.

2 Ülevaade ettevõttest

Käesolevas peatükis antakse ülevaade ettevõtte protsessikesksest juhtimisest ning rikete püstitamise sisenditest.

2.1 Ettevõtte protsessikeskne töökorraldus, protsessi raamistikud

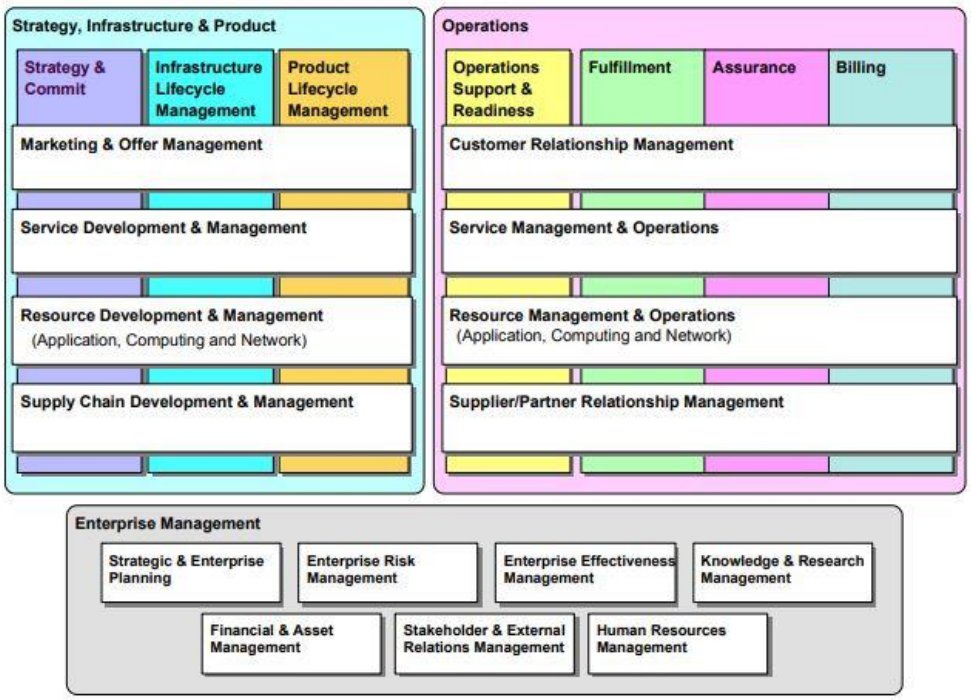
Ettevõtte funktsionaalset juhtimist toetab protsessikeskne töökorraldus, mis tegeleb struktuuriüksusi läbivate töövoogude väljatöötamise ja juurutamisega koostöös ning kokkuleppel vastavate struktuuriüksuste juhtidega. Protsessikeskse töökorralduse toimimise eest vastutab ettevõtte juhtkond ning protsessijuhtimise juhtrühm. Ettevõtte funktsionaalne struktuur toetab ettevõtte protsessipõhist kvaliteedijuhtimissüsteemi. Funktsionaalsete juhtide pädevusega viiakse ettevõtte töötajateni arusaam ettevõtte kvaliteedijuhtimissüsteemi olulisusest ning klientide ja omanike soovidest ning ootustest. Toetus realiseerub ettevõtte funktsionaalsete juhtide ja protsessijuhtide vahel protsesside sujuvaks toimimiseks sõlmitud kokkulepete ning nende täitmise kaudu. Pidev protsessijuhtimise ülevaatus toimub juhtkonnas. Informatsiooni kokkulepetest ja otsustest jagatakse kõigile ettevõtte juhtkonna liikmetele. [3]

Protsessijuhtimise kaudu loob ettevõte väärtust klientidele ja töötajatele, kes vajavad lihtsat, kvaliteetset ning tõhusat töökorraldust, mida aidatakse luua, pakkudes süsteemseid töökorralduslikke lahendusi. [3]

Protsesside klassifikatsioon toetub telekommunikatsiooniettevõtete opereerimisskeemi *Telecom Operations Map* versioonile eTOM (*Enhanced Telecom Operations Map*) [3].

eTOM raamistik võimaldab telekommunikatsiooni ja IT-ettevõtetel olla oma tegutsemises võimalikult efektiivne ja konkurentsivõimeline äriprotsesside rakendamise kaudu. Kategoriseeritud ja selgelt arusaadavad protsessid üle ettevõte aitavad leida ühist keelt erinevate üksuste vahel.

Järgnevalt on esitatud eTOMi 1. taseme protsessijoonis:



Joonis 1. eTOM 1. taseme protsessid [4]

Antud raamistik on hierarhiline kataloog võtmeäriprotsessidest, mis on vajalikud teenusele orienteeritud äri juhtimiseks. Kontseptuaalsel tasemel on raamistikul kolm tähtsat suunda, mis peegeldavad ettevõtte põhifookuseid [5]:

- Strateegia, infrastruktuur ja toode
- Teenuse haldus
- Ettevõtte juhtimine

Ettevõttes on infotehnoloogiateenuste haldamisel juurutatud maailma parima praktikana tunnistatud ITILi (*IT Infrastructure Library*) metoodikaga kooskõlas olevaid teenuste haldamise põhimõtteid. Nende rakendamise eesmärk on tagada erinevate pakutavate teenuste osas terviklik ja kliendi äriprotsesse toetav teenuste haldus. Lähtudes ITILi põhimõtetest on kokku lepitud vastavate tegevuste paiknemine protsessikaardil ning seosed protsesside vahel. [3]

ITIL on enim levinud raamistik maailmas, mis pakub süstemaatilist lähemist IT teenuse haldamisele nii äri- kui kliendivaates. ITILi kasutamine aitab saavutada edu ning tuua kasu alljärgnevates punktides [6]:

- Kasutajate ja klientide rahulolu

- Teenuse parem kättesaadavus
- Kulude kokkuhoid optimeeritud tegutsemise kaudu
- Kiirem uute teenuste toomine turule
- Otsuste tegemise lihtsustamine ja riskide hajutamine

ITIL raamistik hõlmab kogu teenuse elutsüklit. Selle kolmandas versioonis on terviklik elutsükkel jaotatud järgmiselt [6]:

- Teenuse strateegia (*Service Strategy*)
- Teenuse kavandamine (*Service Design*)
- Teenuse opereerimine (*Service Operation*)
- Teenuse üleminek (*Service Transition*)
- Kestev teenuse parendamine (*Continual Service Improvement*)

Bakalaureusetöös keskendub autor ettevõtte teenuste opereerimise protsessigruppi kuuluvatele intsidendihalduse jaoks vajalike võrguintsidendi kahtluste menetlemisele ning vastava protsessi optimeerimisele.

2.2 Intsidendihalduse protsess ja selle seosed teiste teenuste opereerimise protsessidega

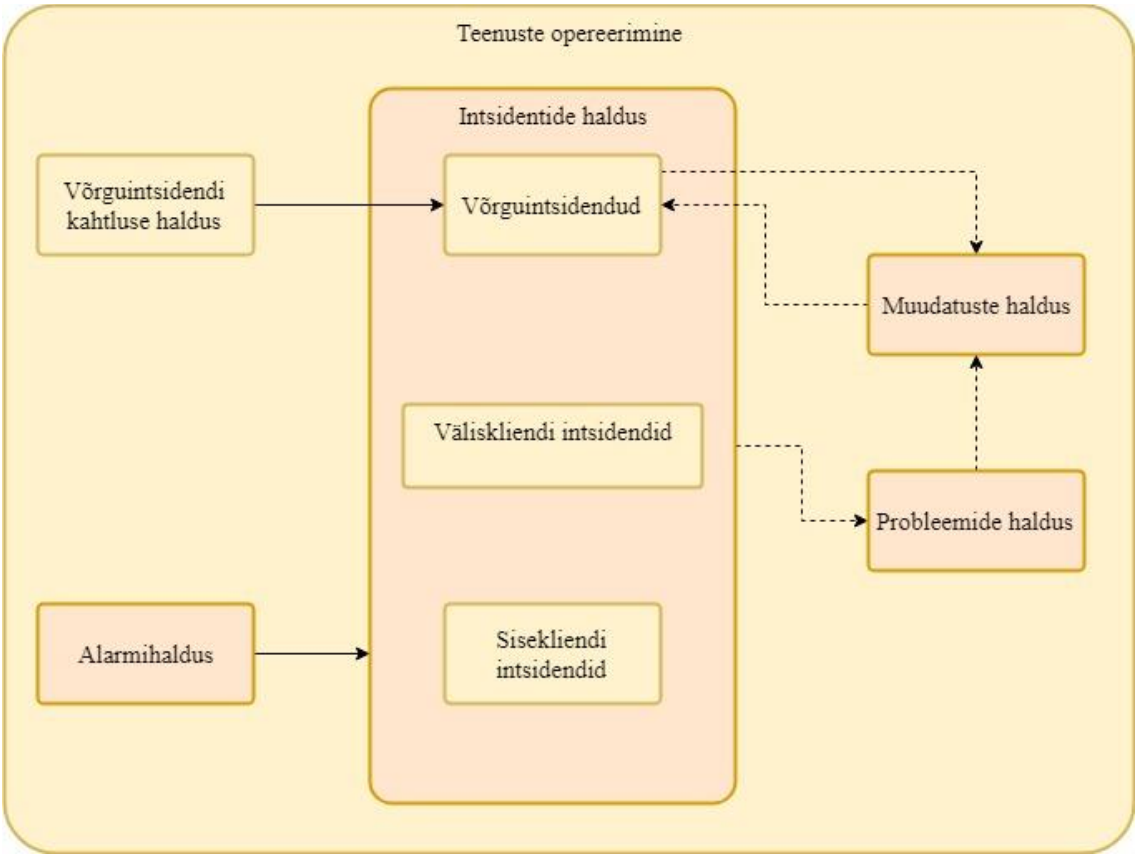
Intsidendihaldus on protsess, mis vastutab kõikide intsidentide kogu elutsükli haldamise eest. Intsidendihalduse protsessi esmane eesmärk on taastada teenus kasutajatele võimalikult kiiresti ning etteantud SLA (*Service Level Agreement*, teenustase) aja sees. Intsidendihaldus on mitmekihiline. Eristatakse võrguintsidente, väliskliendi intsidente ning sisekliendi intsidente.

Intsidendihaldus kuulub teenuste opereerimise protsesside hulka. Intsidendiprotsessi käivitamiseks vajalikud sisendid tulevad sündmuste haldusest ning pöördumistest. Sündmuste halduse (alarmide halduse) protsessi raames fikseeritakse automaatsete ning eelhäälestatud monitooringu süsteemide kaudu anomaaliad ning püsiva või korduva

anomaalia korral käivitatakse intsidendihalduse protsess. Intsidendihalduse protsessi teiseks sisendiks on pöördumine, siin on võimalikud erinevad variandid – telefonikõne, e-mail, veebivorm.

Lisaks kuuluvad teenuste opereerimise protsesside gruppi muudatuste haldus ja probleemide haldus. Muudatuste teostamise ajal võivad tekkida intsidendid, vahel on intsidendi lahendamise käigus vajalik teostada muudatus (tavaliselt erakorraline muudatus). Intsidendi lahendamise käigus võib tekkida olukord, kus intsidendi põhjus pole teada või intsidendi juurpõhjuse likvideerimine nõuab aega. Sellise olukorra kõrvaldamiseks on võimalik püstitada probleem, millega lahendamine toimub probleemide halduse raames. Probleemi lahedamise käigus võib tekkida vajadus muudatuse järele.

Teenuste opereerimise gruppi kuuluvad protsessid ja nendevahelised seosed on esitatud järgmisel joonisel:



Joonis 2. Teenuste opereerimise gruppi kuuluvad protsessid ja nendevahelised seosed

3 Olemasoleva äriprotsessi analüüs

Antud peatükis analüüsib autor hetkel kehtiva võrguintsidendi kahtluse menetlemise protsessi. Töötulemus esitatakse graafiliselt ning sõnalise kirjeldusega. Seejärel tuvastab autor selle protsessi kitsaskohad ning esitab nende parendusettepanekud.

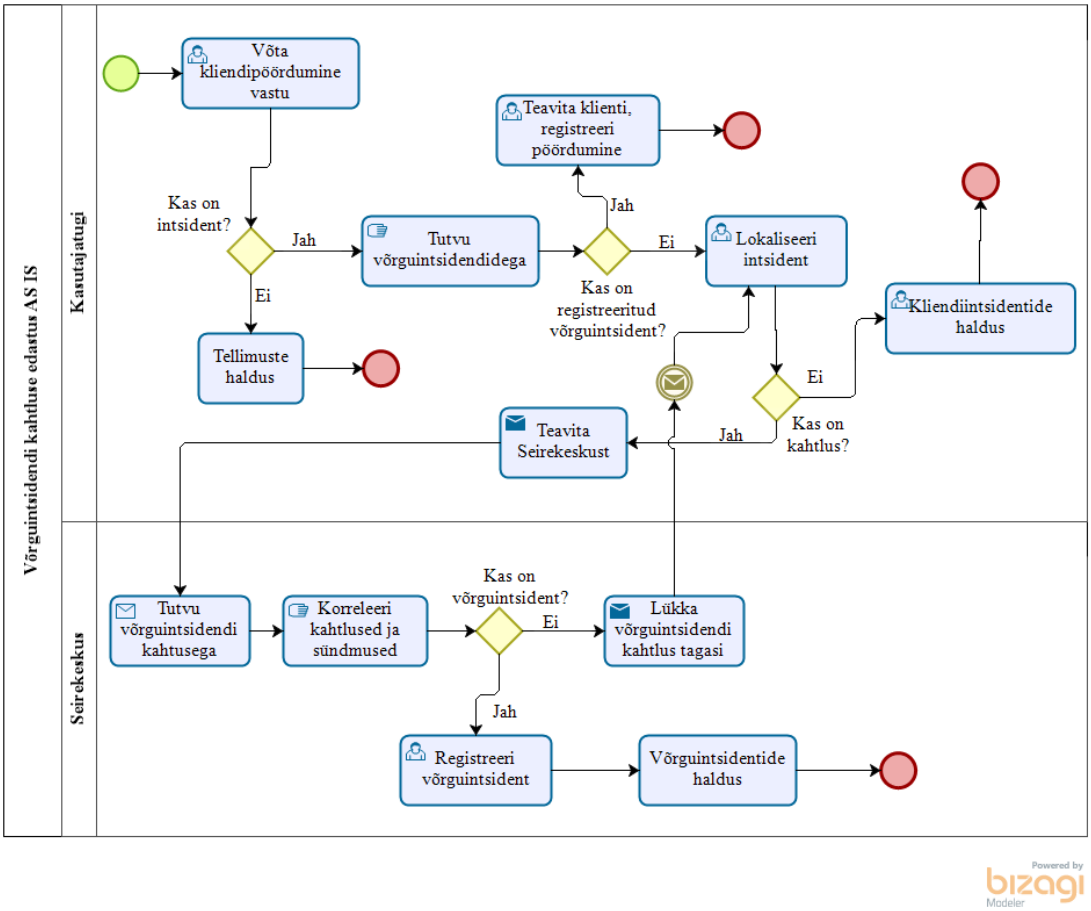
3.1 Võrguintsidendi kahtluse menetlemise olemus

Võrguintsidendi kahtluse menetlemise protsess käsitleb intsidendihalduse protsessis olevaid pöördumisi. Pöördumised võivad tulla erinevate kanalite kaudu – põhiliselt kliendipöördumiste kaudu. Võrguintsidendi kahtlus viitab häirele teenuse töös, mille põhjus ning ulatus pole selge. Võrguintsidendi kahtluse menetlemise protsessi käigus analüüsitakse saadud pöördumised, korreleeritakse need teiste võrguintsidendi kahtlustega, intsidentidega või sündmustega, mis ei ole veel registreeritud intsidendina. Võrguintsidendi kahtluse menetlemise protsessi väljunditeks on tuvastatud võrguintsident või kliendiintsident.

Võrguintsidendi kahtlus püstitatakse teenusega seotud mure korral, tavaliselt kliendipöördumise alusel. Kliendipöördumise ajal tutvub Kasutajatoe töötaja CRM (*Customer Relationship Management*, Kliendisuhete juhtimine) süsteemide kaudu kliendi kohta käiva informatsiooniga, kliendi teenustega ning seotud võrguintsidentidega. Vajadusel pöördub töötaja tehnilistesse süsteemidesse, et kontrollida ühendust või teenust. Võrguintsidendi kahtluse korral teavitab Kasutajatoe töötaja Seirekeskust, kasutades selleks e-maili rakendust. Suurema kahtluse korral on võimalik edastada kahtlus ka telefoni teel.

3.2 Olemasoleva äriprotsessi kaardistus (AS IS)

Järgnevalt on graafiliselt esitatud optimeerimata võrguintsidendi kahtluse menetlemise protsess.



Joonis 3. Võrguintsidendi kahtluse menetlemise protsess AS IS

Võrguintsidendi kahtluse menetlemise protsessi käivitab kliendipöördumine. Kliendipöördumised võivad olla erineva sisuga: tellimus ja infoküsimine, tehniline küsimus.

Kasutajatoe töötaja võtab kliendipöördumise vastu ning tuvastab, milline on kliendi vajadus. Kui kliendil on küsimus teenuse informatsiooni või selle teenuse tellimise kohta, lahendatakse kliendi pöördumine Tellimuste halduses. Kui tegemist on aga teenuse toimimise häirega, algab intsidendi tuvastamine.

Algul tutvub Kasutajatoe töötaja juba töös olevate võrguintsidentidega, mis on juba Seirekeskuse poolt registreeritud. Kui tegemist on võrguintsidendiga, teavitab Kasutajatoe töötaja klienti võrguintsidendist ning registreerib pöördumise süsteemis. Registreeritud ning lahenduses oleva võrguintsidenti korral lõpeb kliendipöördumise menetlemine võrguintsidendi kohase informatsiooni jagamisega kliendile.

Juhul, kui võrguintsident pole veel tuvastatud ning registreeritud, alustab Kontaktikesksuse töötaja intsidendi lokaliseerimist, kasutades erinevaid süsteeme ja juhendeid. Kui analüüsi käigus ei teki kahtlust, et tegemist on võrguintsidendiga, lahendab töötaja kliendipöördumise Kliendiintsidentide halduse protsessis.

Kui intsidendi lokaliseerimisel tekib töötajal kahtlus, et tegemist võib olla võrguintsidendiga, siis saadab ta teavituse e-maili teel Seirekeskusele. Seejärel jääb kliendipöördumine ootama vastust. Kiirema vastuse saamiseks helistab töötaja Seirekesksusele.

Seirekeskuse töötaja tutvub kahtlusega, lugedes saadetud e-maili. Seejärel korreleerib töötaja kahtluse tuvastatud sündmustega või teiste saabunud kahtlustega. Vajadusel teostab töötaja kahtluse lisakontrolli, et tuvastada võrguintsident. Kui kahtlus on tõene, registreerib Seirekeskuse töötaja võrguintsidendi ning saadab vajalikud teavitused Võrguintsidentide halduse protsessi sees.

Juhul, kui võrguintsidenti ei ole tuvastatud, koostab Seirekeskuse töötaja vastuse, milles lükkab võrguintsidendi kahtluse tagasi. Seejärel alustab Kasutajatoe töötaja intsidendi lokaliseerimist uuesti, kasutades erinevaid süsteeme ja juhendeid. Kliendiintsidendi tuvastamisel jätkub protsess Kliendiintsidentide halduses. Kasutajatoe töötaja saab uuesti saata võrguintsidendi kahtluse Seirekeskuse poole, juhul kui uuesti lokaliseerimise jooksul tekkib uus kahtlus või tuleb lisainformatsioon kliendi poolt, mis viitab võrguintsidendile.

3.3 Analüüsitava äriprotsessi kitsaskohad ja parendusettepanekud

Järgnevalt on esile toodud tuvastatud kitsaskohad, mis tulid välja võrguintsidendi kahtluse menetlemise protsessi analüüsi käigus.

Protsessi analüüsi käigus selgus, et mitmed tegevused tehakse erinevates süsteemides eraldi ning süsteemide vahel puudub liidestamine. Andmed kliendi teenuste kohta on leitavad ühes süsteemis ning täiendav diagnostika võib toimuda juba järgmises süsteemis. Olemasolevad võrguintsidendid on leitavad erinevatel vahelehtedel diagnostika ja võrguintsidentide kuvamissüsteemis. Lairiba ühenduste kohta on võimalik kuvada informatsiooni võrguintsidentide kohta CRM süsteemis. Võrguintsidendi kahtlusest võrguintsidendi registreerimine teostatakse käsitsi ehk pole võimalik lihtsalt ja mugavalt

kasutada e-maili rakenduses olevat infomatsiooni. Võrguintsidendi kahtluse menetlemise kvaliteeti pole võimalik automaatselt mõõta. Võrguintsidendi kahtluste menetlemise kontrolli jaoks kulutatakse iganädalaselt analüütikute aega. Kontroll toimub e-maili rakenduses e-mailide ülevaatamise teel ning selleks peab analüütik lugema nii püstitatud võrguintsidendi kahtluseid kui ka püstitatud kahtluste vastuseid. Püstitatud võrguintsidendi kahtlused ning vastused nendele seotakse analüüsi käigus käsitsi. Kontrolli tulemused esitatakse iganädalasel operatiivkoosolekul võrguintsidentide ühe sisendina.

Võrguintsidendi kahtluse edastamine ja tagasilükkamine e-maili teel ei võimalda koondada ühte kohta kõik saadetud, kinnitatud või tagasilükatud võrguintsidendi kahtlused. Selliselt suureneb võimalus jätta olulist informatsiooni märkamata ning info puudumise tõttu langetada pöördumiste lahendamisel vale otsus.

Võrguintsidendi kahtluse menetlemiseks on loodud e-posti aadress, mis on tehniliselt lahendatud liikmete listina, kus on üle 200 liikme Kasutajatoest, Seirekeskusest ja teistest üksustest. Vaatamata listi suurusele pole informatsioon kättesaadav kõikide töötajate jaoks, kes vajavad informatsiooni võrguintsidentide ning võrguintsidendi kahtluste kohta. Kasutusel oleval e-maili aadressil on ka teine kasutamise eesmärk. Kasutajatoe töötajad kasutavad aadressi teistelt listi liikmetelt pärimiseks, kas sarnaseid pöördumisi on ka nendele laekunud. Selliselt võib tekkida olukord, kus ei ole selgelt aru saada, kas tegemist on võrguintsidendi kahtlusega või mitte.

Liidestamise puudumine seab ohtu ka võrguintsidendi kahtluse sisulise kvaliteedi. Kirja koostamisel võib oluline info CRM süsteemist või diagnostika vahenditest jääda lisamata, mis vähendab kogu protsessi efektiivsust.

Järgnevalt toob autor tuvastatud kitsaskohad kokkuvõtvalt uuesti välja:

- Liidestamise puudumine erinevate süsteemide vahel
- Automaatse võrguintsidendi kahtluse menetlemise kvaliteedi kontrolli puudumine
- Ühtse võrguintsidendi kahtluste baasi puudumine, kuhu oleks koondatud kõik püstitatud võrguintsidentide kahtlused ning nende vastused

- Kasutusel oleva tehnilise lahenduse ebamugavus ei võimalda kõikidel osapooltel infot saada
- Ebaefektiivne analüütikute ressursi kasutamine

Parendusettepanekud:

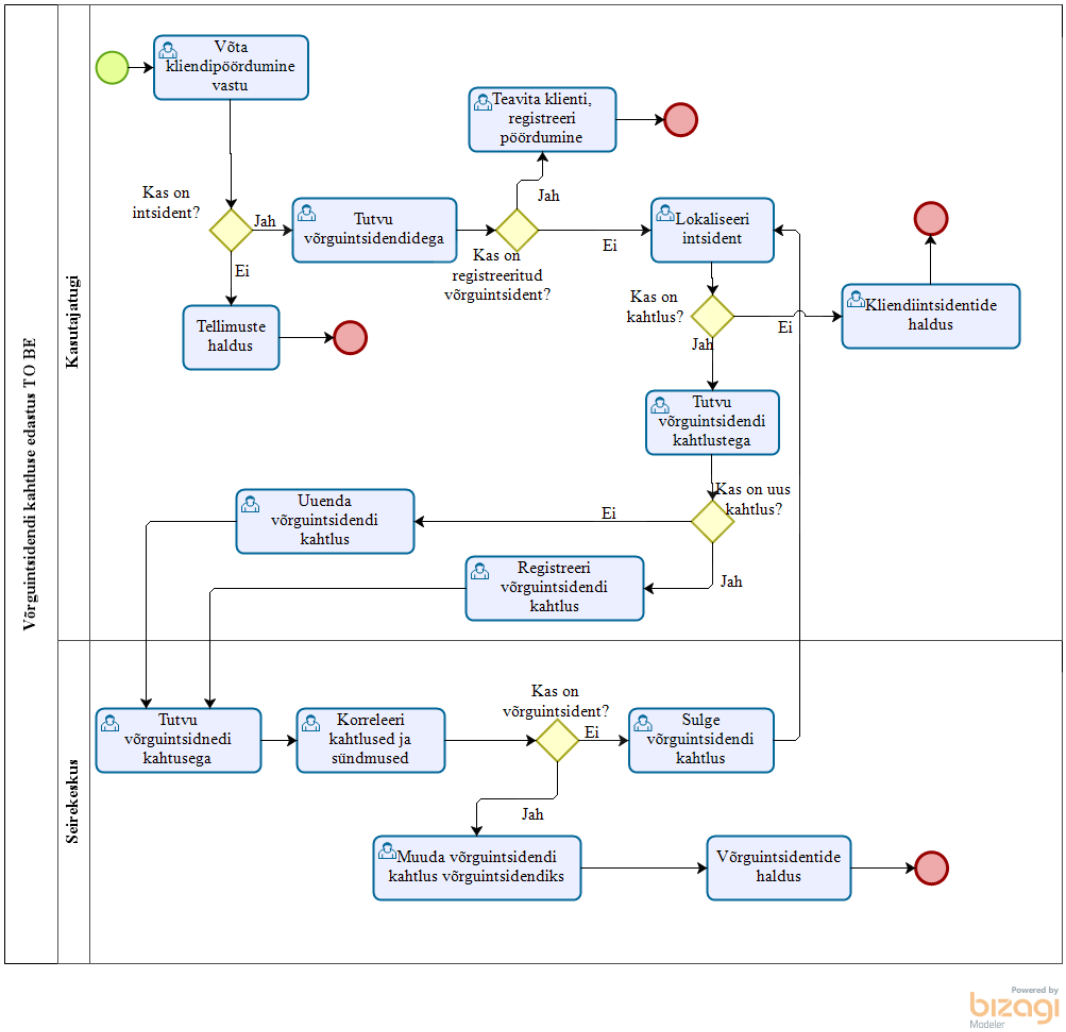
- Uue võrguintsidendi kahtluse menetlemise süsteemi loomine, mis oleks kasutatav kõikide osapoolte poolt ning aitaks võrguintsidendi kahtluse menetlemise tegevused viia süsteemi, loobudes võrguintsidendi kahtluste menetlemisest e-maili teel
- Uue süsteemi liidestamine olemasolevate süsteemidega
- Automaatse võrguintsidendi kahtluste menetlemise kvaliteedi aruande loomine

4 Äriprotsessi optimeerimine

Antud peatükis toob autor välja tuleviku protsessi. Töötulemus esitatakse graafiliselt ning sõnalise kirjeldusega. Seejärel toob autor esile ka ärireeglid ning võrguintsidendi kahtluste menetlemise kvaliteedi aruandluse mõõdikud.

4.1 Optimeeritud äriprotsessi kaardistus (TO BE)

Järgnevalt on graafiliselt esitatud optimeeritud protsess, mille toetamiseks on vajalik arendada uus tehniline lahendus.



Joonis 4. Võrguintsidendi kahtluse menetlemise protsess TO BE

Uus võrguintsidendi kahtluse menetlemise protsess on välja töötatud parendusettepanekute alusel. Uue süsteemi loomine võimaldab muuta võrguintsidendi kahtluse menetlemist efektiivsemaks.

Endiselt algab protsess kliendipöördumisega, mille menetlemine toimub Kontaktikeskuses. Kui kliendipöördumine on seotud intsidendiga, tutvub Kasutajatoe töötaja töös olevate võrguintsidentidega. Pöördumisega seotud võrguintsidendi puudumisel jätkab Kasutajatoe töötaja intsidendi lokaliseerimist. Kui viimase tegevuse käigus tekib Kasutajatoe töötajal kahtlus, et tegemist võib olla võrguintsidendiga, siis tutvub ta juba registreeritud võrguintsidendi kahtlustega. Samalaadse võrguintsidendi kahtluse puhul uuendab ta võrguintsidendi kahtlust. Seotud võrguintsidendi kahtluse puudumisel sisestab uue võrguintsidendi kahtluse.

Seirekeskuse töötaja võtab uues süsteemis kahtluse vastu ning jätkab kahtluste ja sündmuste korreleerimisega. Kui eelmise tegevuse käigus ei avasta Seirekesksuse töötaja võrguintsidenti, sulgeb ta kahtluse. Kahtluse sulgemise järel alustab Kasutajatoe töötaja intsidendi lokaliseerimist uuesti, kasutades erinevaid süsteeme ja juhendeid. Kliendiintsidendi tuvastamisel jätkub protsess Kliendiintsidentide halduses. Kasutajatoe töötaja saab uuesti saata võrguintsidendi kahtluse Seirekeskuse poole, juhul kui uuesti lokaliseerimise jooksul tekib uus kahtlus või tuleb lisainformatsioon kliendi poolt, mis viitab võrguintsidendile.

Kui kahtlus on tõene, muudab Seirekesksuse töötaja kahtluse võrguintsidendiks ning edasine menetlemine jätkub võrguintsidentide halduse protsessi sees.

4.2 Ärireeglid

Järgnevalt on esitatud ärireeglid:

- Iga võrguintsidendi kahtlus, mis on sisestatud Kasutajatoe töötaja poolt ning mille staatus on „uus“, peab olema vastu võetud ning staatus muudetud „uurimisel“ peale hiljemalt 15 minuti jooksul alates selle sisestamise ajast

- Iga „uurimisel“ staatuses oleva võrguintsidendi kahtluse kohta peab olema otsus tehtud ning sõltuvalt otsusest muudetud staatus „võrguintsident“ või „korras“

peale hiljemalt 1 tunni jooksul alates selle võrguintsidendi kahtluse sisestamise ajast

- Iga võrguintsidendi kahtlus, mis sisestatakse süsteemis, on logitav kesksesse logisüsteemi ning kättesaadav aruandluse keskkonna jaoks
- Iga võrguintsidendi kahtluse staatuse muudatus on logitav kesksesse logisüsteemi ning kättesaadav aruandluse keskkonna jaoks
- Kõik võrguintsidendi kahtlused staatuses „uus“, „uurimisel“, „intsident“ on kuvatud süsteemi kasutajatele
- Süsteemi kaudu on võimalik vaadata ka „korras“ staatuses olevaid võrguintsidendi kahtluseid 1 kuu tagasiulatavalt
- Võrguintsidendi kahtlus staatuses “Võrguintsident“ läheb automaatselt „Korras“ staatusesse seotud võrguintsidendi sulgemisel.

4.3 Võrguintsidendi kahtluse menetlemise kvaliteet

Uue süsteemi kasutusele võtmine avab võimaluse luua võrguintsidendi kahtluse menetlemise kvaliteedi aruande, mille saaks võtta kasutusele iganädalastel operatiivkoosolekutel ning mis muudaks analüütikute ressursi kasutamist efektiivsemaks. Antud aruanne sisaldaks nädala jooksul püstitatud võrguintsidendi kahtluseid ning nende vastuseid. Samuti annaks aruanne ülevaate, kui kiiresti olid võrguintsidendi kahtlused vastu võetud ning vastatud.

Ärireeglite täitmise jälgimiseks on vaja seada võrguintsidendi kahtluse menetlemise protsessile alljärgnevad KPI-d (*Key Performance Indicator*, Tulemuslikkuse võtmemõõdik):

- Vähemalt 90% sisestatud võrguintsidendi kahtlustest on 15 minuti jooksul vastu võetud
- Vähemalt 90% sisestatud võrguintsidendi kahtlustele on 1 tunni jooksul vastatud

5 Uus süsteem „Võrguintsidendi kahtlus“

Antud peatükis kirjeldab autor uue võrguintsidendi kahtluse menetlemise süsteemi. Autor toob välja süsteemi nõuded, esitab pakutava uue süsteemi prototüübi ning selle süsteemi liidestamise teiste süsteemidega.

5.1 Süsteemi nõuded

Võrguintsidendi kahtluse menetlemise kiiruse ja efektiivsuse tõstmiseks pakub autor uue süsteemi loomist. Uus süsteem peab toetama TO-BE protsessi.

Uue süsteemi funktsionaalsed nõuded:

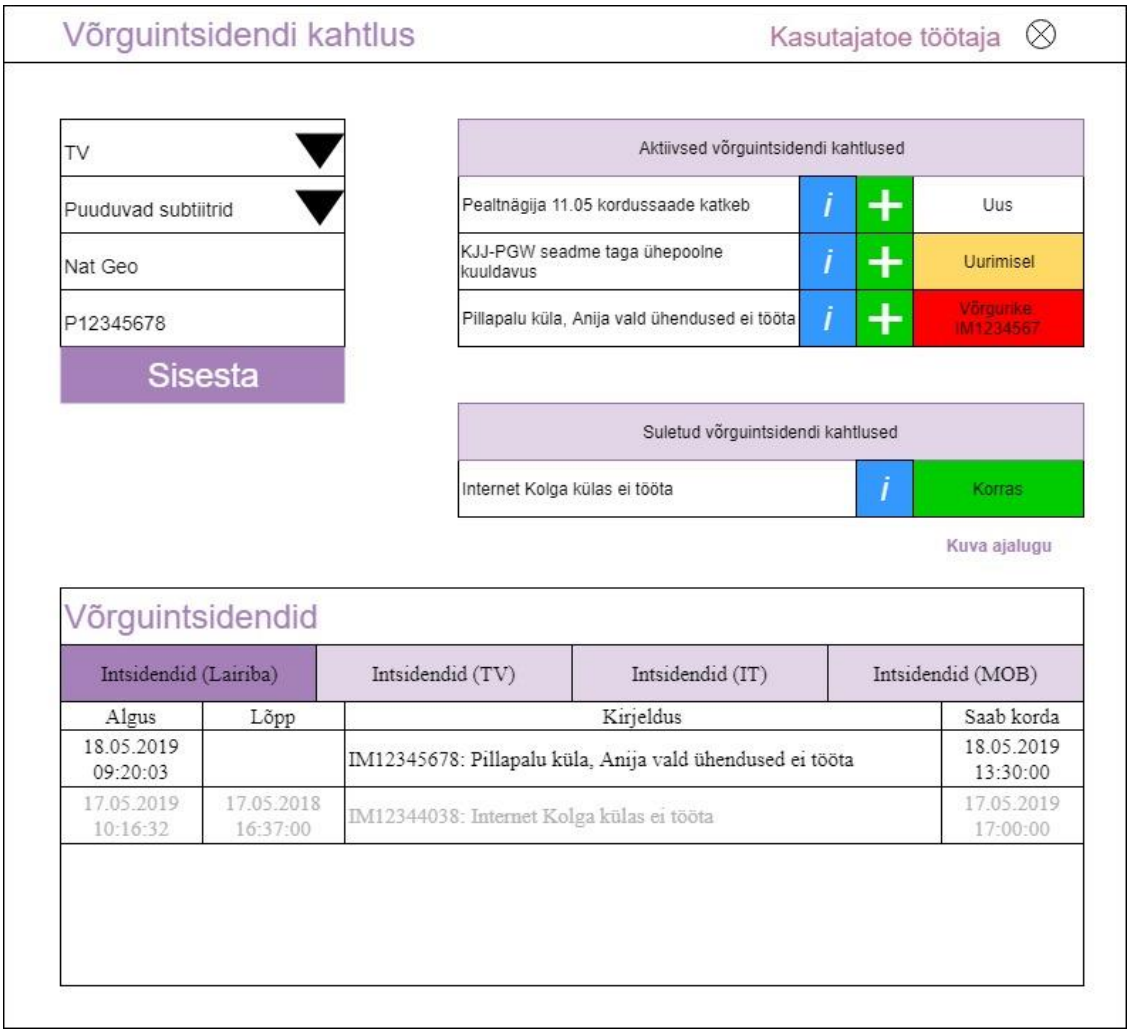
- Süsteem peab võimaldama sisestada võrguintsidendi kahtlust Kasutajatoe töötajatel
- Süsteem peab võimaldama uue sarnase sisuga võrguintsidendi kahtluse sidumist juba sisestatud võrguintsidendi kahtlusega
- Süsteem peab võimaldama püstitatud võrguintsidendi kahtluse staatust muuta Seirekeskuse töötaja poolt
- Süsteem peab võimaldama püstitatud võrguintsidendi kahtlust muuta võrguintsidendiks
- Süsteem peab logima kõik sisestatud võrguintsidendi kahtlused ning kõik toimingud, mis sisestatud võrguintsidendi kahtlustega tehakse, näiteks staatuse muutmine
- Süsteem peab kuvama aktiivseid võrguintsidendi kahtluseid
- Süsteem peab kuvama viimase 1 kuu jooksul suletud võrguintsidendi kahtluseid
- Süsteem peab kuvama töös olevaid ning võrguintsidentide kuvamissüsteemis kuvatavaid intsidente

Uue süsteemi mittefunktsionaalsed nõuded:

- Kättesaadavus. Süsteem peab vastama vähemalt ärikriitilise teenuse tasemele.
- Laiendatavus. Süsteem peab olema suuteline töötama ka võrguintsidendi kahtluste sisestamise mitmekordsel kasvul. Samuti peab süsteemi saama laiendada uue funktsionaalsusega nii, et olemasolev funktsionaalsus säiliks ega vajaks suurt ümbertegemist.
- Kiirus. Süsteem peab reageerima päringutele maksimaalselt 3 sekundi jooksul.
- Jõudlus. Süsteem peab olema suuteline töötama ka juhul, kui kasutajate hulk on suur.
- Ligipääsetavus. Süsteem peab olema kättesaadav 24/7.
- Juurdepääsetavus. Süsteemi kasutajad peavad saama ligi tööarvutite kaudu ja kindlate ligipääsuparoolide kaudu.
- Vastavus standarditele. Süsteemi arendustegevused ja tehnilised lahendused peavad vastama standarditele (ettevõttes kokkulepitud arhitektuuri raamistikule).

5.2 Kasutajatoe töötaja kasutajaliidese prototüüp

Järgnevalt on esitatud uue süsteemi kasutajaliidese prototüüp Kasutajatoe töötaja rollile. Rolli valimisel lähtus autor kasutajate arvust, kes täidavad antud rolli.



Joonis 5. Uus süsteem: Kasutajatoe töötaja vaade

Prototüübil on esitatud Kasutajatoe töötaja vaade, mis avaneb pärast sisse logimist. Ülemises reas on kuvatud kasutaja nimi ning nime kõrval asub välja logimise nupp.

Kasutajaliidese prototüübi vasakul poolel asub võrguintsidendi kahtluse sisestamise vorm, kus osade väljade täitmisel kasutatakse eeldefineeritud valikuid ning osad väljad saab täita, sisestades vaba väärtuse. Teise väärtuse valimine sõltub eelmisest ning osade teenuste puhul võib valikute puu olla ka kolmetasandiline.

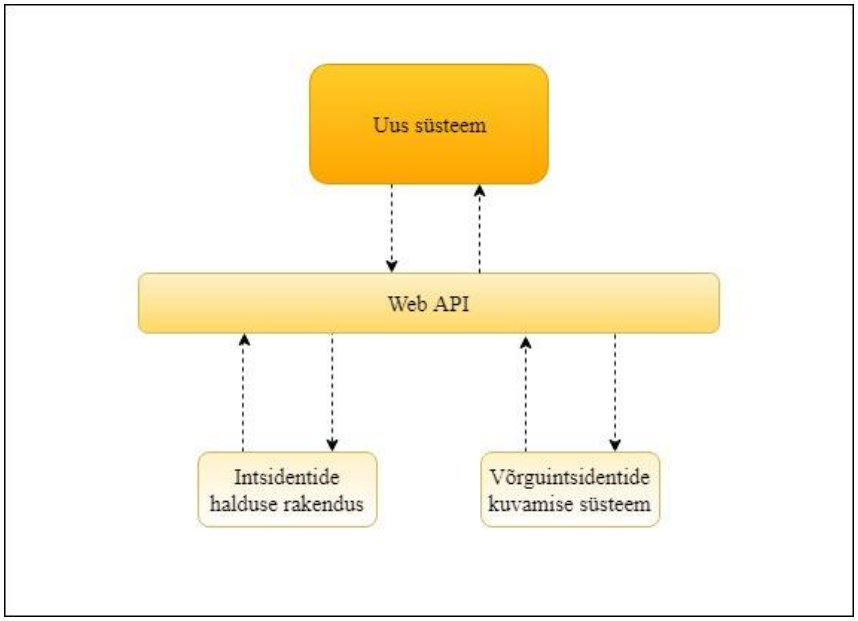
Kasutajaliidese prototüübi paremas osas on kuvatud sisestatud võrguintsidendi kahtlused. Üleval pool on kuvatud staatuse järjekorras aktiivsed võrguintsidendi kahtlused. Kirjelduse järel asuvad nupud „i“ ja „+“, mille kaudu saab vaadata võrguintsidendi kahtluse täpsemat sisu ning siduda uus pöördumine sama võrguintsidendi kahtlusega. „+“ nuppu vajutamisel avaneb hüppeaknas võrguintsidendi kahtluse sisestamise vorm. Aktiivsete võrguintsidendi kahtluste all on kuvatud värskelt suletud võrguintsidendi

kahtlused, mille staatus on korras. „Kuva ajalugu“ nuppu vajutades ilmub ajalugu ühe kuu ulatuses. Kandeid kuvatakse 25 kaupa ning alla tekib navigatsioonirida.

Võrguintsidendi kahtluse mooduli all kuvatakse samal lehel võrguintsidendid. Info pärineb võrguintsidentide kuvamissüsteemist.

5.3 Uue süsteemi liidestamine

Järgneval joonisel on toodud uue süsteemi liidestamine olulisemate süsteemidega. Liidestamine teostatakse Web API kaudu (*Web Application Programming Interface*, veebipõhine rakendusliides). Lisaks liidestatakse uus süsteem ka keskse logisüsteemiga ning aruandluse süsteemiga.



Joonis 6. Uue süsteemi liidestamine

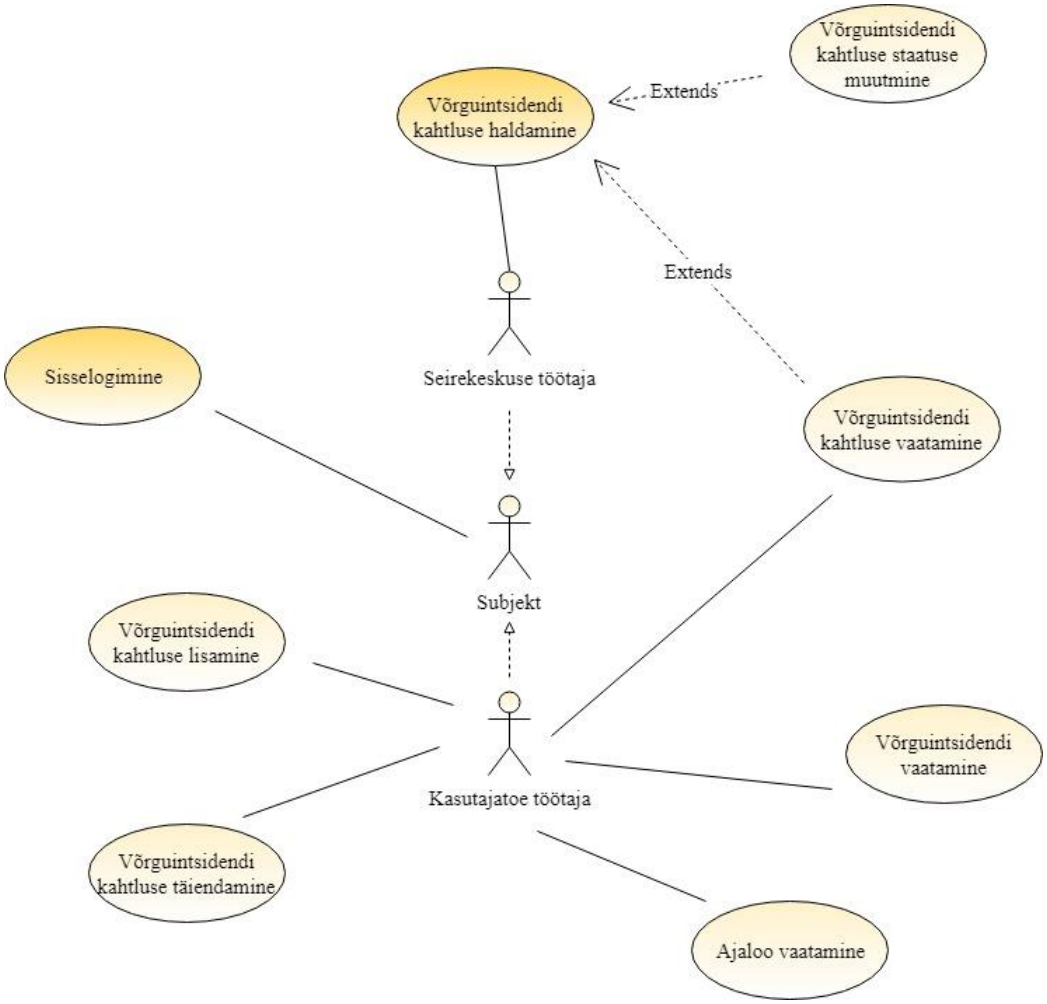
Võrguintsidendi kahtluse muutmisel võrguintsidendiks liigub vastav sõnum uuest süsteemist intsidentide halduse rakendusse Web API kaudu. Saadetud sõnum genereerib intsidentide halduse rakenduses uue võrguintsidendi ning tagasi läheb sõnum Web API kaudu, et uus võrguintsident on loodud. Sõnumiga kaasa tuleb ka unikaalne identifikaator, millega seotakse võrguintsidendi kahtlus ja võrguintsident. Sarnaselt liigub informatsioon võrguintsidentide kohta intsidentide halduse rakendusest võrguintsidentide kuvamise süsteemi Web API kaudu.

6 Uue süsteemi kasutusjuhud ja võrguintsidendi kahtluse olekud

Antud peatükis kirjeldab autor kasutusjuhud, mis annavad ülevaate tegevustest, mida uue süsteemi kasutajad saavad teha. Seejärel esitab autor võrguintsidendi kahtluse olekudiagrammi.

6.1 Kasutusjuhtude diagramm

Järgnevalt on esitatud kasutujuhtude diagramm.



Joonis 7. Kasutusjuhtude diagramm

6.2 Kasutusjuhud laiendatud formaadis

Kasutusjuht: Sisselogimine

Tegutsejad: Kasutajatoe töötaja, Seirekeskuse töötaja

Eesmärk: Logida sisse süsteemi

Kirjeldus: Subjekt sisestab domeeni kasutajanime ja parooli ning vajutab „Logi sisse“

Eeltingimused: Subjekt on avanud uue süsteemi pealehte

Järeltingimused: Subjekt on sisse logitud

Stsenaarium:

Kasutaja	**Süsteem**
Sisestab domeeni kasutajanime ja parooli ning vajutab „Logi sisse“	Valideerib sisestatud kasutajanime ja parooli. Kui andmed on õiged, siis avaneb pealeht rollile vastavate õigustega. Vastasel juhul kuvab veateadet

Alternatiivid: Parooli taastamist võib teha sisemise arvutiabi kaudu või kasutades domeeni taastamise portaali

Kasutusjuht: Võrguintsidendi kahtluse haldamine

Tegutsejad: Seirekeskuse töötaja

Eesmärk: Hallata sisestatud võrguintsidendi kahtluseid

Kirjeldus: Seirekeskuse töötaja saab vaadata võrguintsidendi kahtlust ning muuda selle staatust

Eeltingimused: Seirekeskuse töötaja peab olema sisse logitud

Järeltingimused: Vajalikud võrguintsidendi kahtluse haldustegevused on tehtud

Stsenaarium:

Kasutaja	**Süsteem**
Vajutab süsteemis vajalikke nuppe	Kuvab vastavalt vajutatud nuppudele sisu
Teeb vajalikud toimingud	Salvestab muudatused

Alternatiivid: Kui mõned tegevused ebaõnnestuvad, saab jagada informatsiooni võrguintsidendi kahtluste kohta e-maili teel

Kasutusjuht: Võrguintsidendi kahtluse staatuse muutmine

Tegutsejad: Seirekeskuse töötaja

Eesmärk: Muuta sisestatud võrguintsidendi kahtluse staatust

Kirjeldus: Seirekeskuse töötaja saab vastavalt vajadusele muuta sisestatud võrguintsidendi kahtluse staatust. Võrguintsidendi kahtluse staatust „Uus“ on võimalik muuta järgnevate staatustega: „Uurimisel“, Võrguintsident“ või „Korras“. „Uurimisel“ staatusest saab edasi liikuda „Võrguintsident“ või „Korras“ staatusesse. „Võrguintsident“ staatuses võrguintsidendi kahtlus muutub automaatselt „Korras“ staatusesse seotud võrguintsidendi sulgemisel

Eeltingimused: Seirekeskuse töötaja on sisse logitud

Järeltingimused: Võrguintsidendi kahtluse staatus on muudetud

Stsenaarium:

Kasutaja	**Süsteem**

Valib võrguintsidendi kahtluse, mille staatust on vaja muuta	Kuvab võrguintsidendi kahtluse detaile ning avaneb võimalus muuta staatust
Valib soovitud staatuse ning salvestab	Muudab valitud võrguintsidendi kahtluse staatust

Alternatiivid: Kui mõned tegevused ebaõnnestuvad, saab jagada informatsiooni võrguintsidendi kahtluste kohta e-maili teel

Kasutusjuht: Võrguintsidendi kahtluse vaatamine

Tegutsejad: Kasutajatoe töötaja, Seirekesksuse töötaja

Eesmärk: Vaadata võrguintsidendi kahtluse detailvaadet

Kirjeldus: Tegutseja valib võrguintsidendi kahtluse, mille detailvaadet on vaja vaadata, ning vajutab selle võrguintsidendi kahtluse juures olevat nuppu. Vastavalt ligipääsu tasemele avaneb detailvaade. Seirekeskuse töötajal kuvab detailvaatele lisaks süsteem staatuse muutmise valikut

Eeltingimused: Tegutseja on sisse logitud

Järeltingimused: Võrguintsidendi kahtluse detailid on vaadatud

Stsenaarium:

Kasutaja	**Süsteem**
Valib võrguintsidendi kahtluse ning vajutab selle kõrval olevat „i“ nuppu	Kuvab valitud võrguintsidendi kahtluse detailvaadet

Alternatiivid: Juhul, kui tehnilistel põhjustel detailide kuvamine ebaõnnestub, saab uurida infot, kasutades e-maili või telefoni

Kasutusjuht: Võrguintsidendi vaatamine

Tegutsejad: Kasutajatoe töötaja

Eesmärk: Vaadata võrguintsidendi detailvaadet

Kirjeldus: Kontaktikesksuse töötaja valib võrguintsidendi, mille detailvaadet on vaja vaadata ning vajutab selle võrguintsidendi juures olevat viidet. Vastavalt ligipääsu tasemele avaneb detailvaade.

Eeltingimused: Kasutajatoe töötaja on sisse logitud

Järeltingimused: Võrguintsidendi detailid on vaadatud

Stsenaarium:

Kasutaja	**Süsteem**
Valib võrguintsidendi ning vajutab selle kõrval olevale viitele	Kuvab valitud võrguintsidendi detailvaadet

Alternatiivid: Juhul, kui tehnilistel põhjustel detailide kuvamine ebaõnnestub, saab uurida infot Marvini kaudu või kasutades e-maili või telefoni

Kasutusjuht: Ajaloo vaatamine

Tegutsejad: Kasutajatoe töötaja

Eesmärk: Vaadata võrguintsidendi kahtluste ajalugu

Kirjeldus: Kasutajatoe töötaja vajutab „Vaata ajalugu“ viidet, mille vajutades kuvab süsteem „Korras“ staatuses võrguintsidendi kahtluste listi ning kui listis on üle 25 kirje, siis kuvab ka navigeerimisriba

Eeltingimused: Tegutseja on sisse logitud

Järeltingimused: Võrguintsidendi kahtluste ajalugu on vaadatud

Stsenaarium:

Kasutaja	**Süsteem**
Vajutab „Vaata ajalugu“ viidet	Kuvab „Korras“ staatuses olevate võrguintsidendi kahtluste listi. Kui listis on rohkem kui 25 kirjet, siis listi alla kuvab süsteem navigeerimisriba
Vajadusel liigub navigeerimisrea kaudu vajalikule lehele	

Alternatiivid: Juhul, kui tehnilistel põhjustel peaks ajaloo kuvamine ebaõnnestuma, saab vaadata ajalugu aruandluskeskkonnast, eeldusel, et töötajal on olemas sellele süsteemile ligipääs

Kasutusjuht: Võrguintsidendi kahtluse täiendamine

Tegutsejad: Kasutajatoe töötaja

Eesmärk: Täiendada juba sisestatud ja „Uus“ või „Uurimisel“ staatuses oleva võrguintsidendi kahtlust uue kliendi pöördumisega, juhul, kui tegemist on seotud võrguintsidendi kahtlusega

Kirjeldus: Kasutajatoe töötaja valib võrguintsidendi kahtluse, mille kohta soovib lisada uue kliendi seotud pöördumise, Vajutades „+“ nupule avaneb võrguintsidendi kahtluse sisestamise vorm

Eeltingimused: Tegutseja on sisse logitud

Järeltingimused: Võrguintsidendi kahtlus on täiendatud uue informatsiooniga, uue pöördumisega

Stsenaarium:

Kasutaja	Süsteem
Valib võrguintsidendi kahtluse ning vajutab selle kõrval oleva „+“ nuppu	Kuvab võrguintsidendi kahtluse sisestamise vormi
Täidab vormi ja vajutab „Lisa“ nuppu	Salvestab uue informatsiooni võrguintsidendi kahtluse sisse

Alternatiivid: Juhul, kui tehnilistel põhjustel võrguintsidendi kahtluse täiendamine ebaõnnestub, saab vajaliku informatsiooni edastada e-maili teel

Kasutusjuht: Võrguintsidendi kahtluse sisestamine

Tegutsejad: Kasutajatoe töötaja

Eesmärk: Sisestada võrguintsidendi kahtlust

Kirjeldus: Tegutseja täidab avalehel oleva vormi ning vajutab „Sisesta“ nuppu. Kõik vormi väljad on kohustuslikud, väljade arv on muutlik, juhul kui eeldefineeritud valikud lähevad kolmetasandiliseks (sõltuvalt valitud valdkonnast ja teenusest)

Eeltingimused: Kasutajatoe töötaja on sisse logitud

Järeltingimused: Võrguintsidendi kahtlus on sisestatud

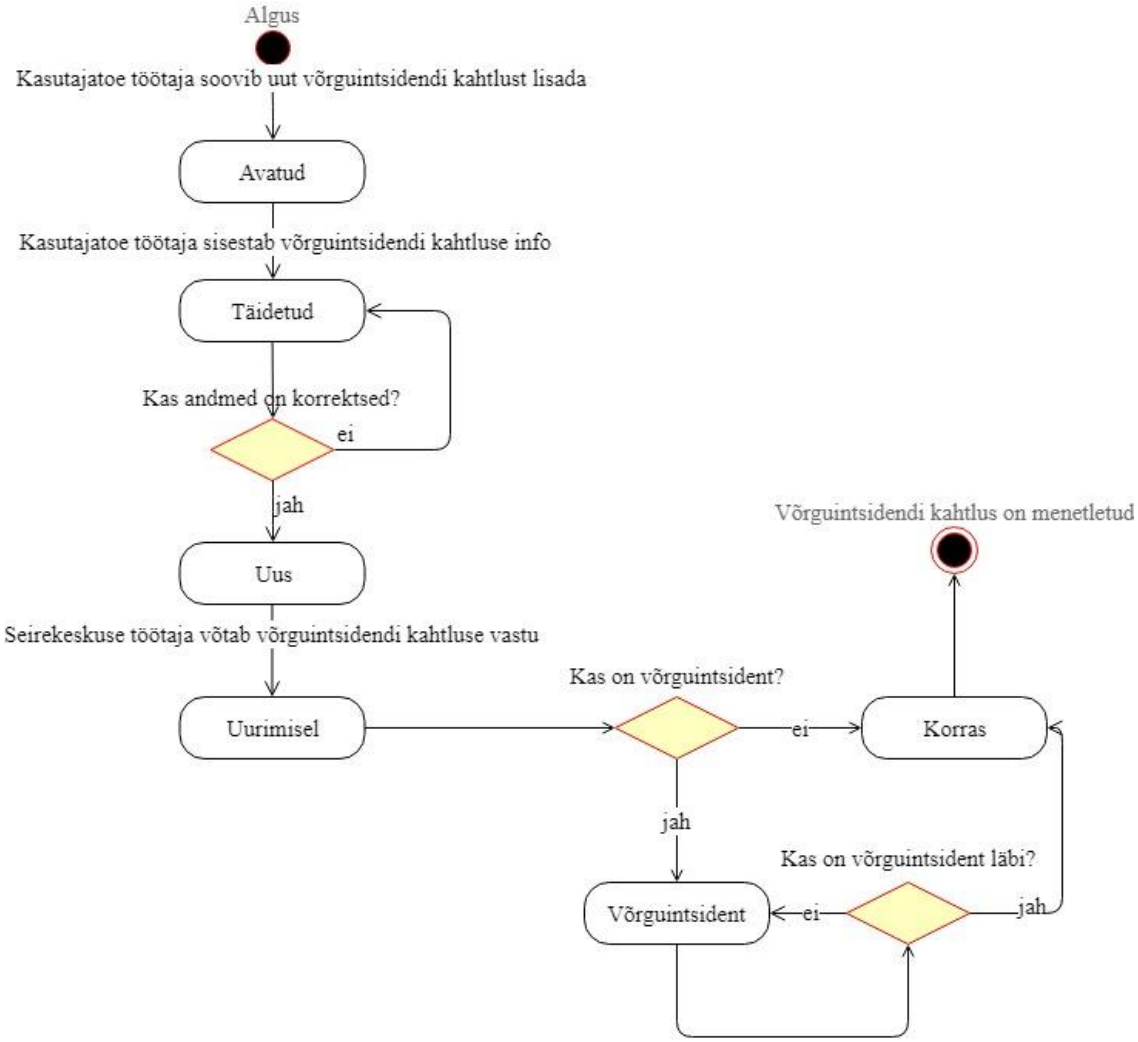
Stsenaarium:

Kasutaja	Süsteem
Osade väljade puhul valib eeldefineeritud valikud ning tekstiväljad täidab vajaliku informatsiooniga. Seejärel vajutab „Sisesta“ nuppu	Salvestab uue võrguintsidendi kahtluse staatusega „Uus“ ning kuvab selle töös olevate võrguintsidendi kahtluste listis

Alternatiivid: Juhul, kui tehnilistel põhjustel uue võrguintsidendi kahtluse sisestamine pole võimalik, edastab võrguintsidendi kahtluse e-maili või telefoni teel

6.3 Võrguintsidendi kahtluse olekudiagramm

Järgnevalt on esitatud võrguintsidendi kahtluse olekudiagramm. Võrguintsidendi kahtlusel võib olla 6 olekut: „Avatud“, „Täidetud“, „Uus“, „Uurimisel“, „Võrguintsident“ ning „Korras“.



Joonis 8. Võrguintsidendi kahtluse olekudiagramm

7 Kokkuvõte

Käesoleva bakalaureusetöö eesmärgiks oli läbi viia võrguintsidendi kahtluse menetlemise protsessi analüüs infotehnoloogia ettevõttes selle protsessi parendamise eesmärgil, dokumenteerida analüüsi tulemused ning tuua välja idee uue süsteemi kohta, mis toetab valitud äriprotsessi parendamist. Lõputöö teoreetilises osas tutvustas autor ettevõttes kasutatavaid teenuse opereerimise ja ärijuhtimise raamistikke.

Töö tulemusena on modelleeritud uus võrguintsidendi kahtluse menetlemise protsess ning uus süsteem, mille kaudu on võimalik hallata võrguintsidendi kahtluseid. Selleks on teostatud valitud äriprotsessi analüüsi, suheldes selles protsessis tegutsejatega ning leitud selle protsessi kitsaskohti ning tehtud parendusettepanekuid.

Töös välja pakutud uue optimeeritud äriprotsessi ja võrguintsidendi kahtluse haldamise süsteemi juurutamine on võetud fookusesse käesoleval aastal. Kokkuvõtvalt võib öelda, et bakalaureusetöös püstitatud eesmärgid said täidetud.

Kasutatud kirjandus

[1] „Bizagi,“ [Võrgumaterjal]. Available: https://www.bizagi.com/.

[2] „Business Process Model and Notation,“ [Võrgumaterjal]. Available: http://www.bpmn.org/.

[3] „Ettevõtte juhtimissüsteemi käsiraamat,“ [Võrgumaterjal]. [Kasutatud 2018].

[4] „Introduction to eTOM,“ [Võrgumaterjal]. Available: https://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-541448.html.

[5] „Business Process Framework (eTOM),“ [Võrgumaterjal]. Available: https://www.tmforum.org/business-process-framework/. [Kasutatud 2018].

[6] „An Introductory overview of ITIL V3,“ [Võrgumaterjal]. Available: http://www.itsmf.org.rs/sites/default/files/itSMF%20ITIL%20V3%20Introduction%20Overview.pdf. [Kasutatud 2018].