УНИВЕРЗИТЕТ „СВ. КИРИЛ И МЕТОДИЈ“- СКОПЈЕ

ФАКУЛТЕТ ЗА ИНФОРМАТИЧКИ НАУКИ
И КОМПЈУТЕРСКО ИНЖЕНЕРСТВО

М-р Југослав Ачкоски

ПРИМЕНА НА СЕРВИСНО ОРИЕНТИРАНА АРХИТЕКТУРА ЗА РАЗВОЈ НА ПРОТОТИП НА ИНФОРМАЦИСКИ СИСТЕМ ЗА РАЗУЗНАВАЊЕ

- докторска дисертација -

Скопје, 2012 година

Ментор:

Вонр. проф. д-р Владимир Трајковиќ
ФИНКИ – Скопје

Комисија за оцена и одбрана:

1. Проф. д-р Драган Михајлов, претседател,
   ФИНКИ – Скопје, Р. Македонија

2. Вонр. проф. д-р Владимир Трајковиќ, ментор,
   ФИНКИ – Скопје, Р. Македонија

3. Доц. д-р Методија Дојчиновски, член,
   Воена академија „Генерал Михаило Апостолски“ – Скопје, Р. Македонија

4. Вонр. проф. д-р Верица Бакева, член,
   ФИНКИ – Скопје, Р. Македонија

5. Доц. д-р Иван Чорбев, член,
   ФИНКИ – Скопје, Р. Македонија

Датум на одбрана:

Датум на промоција:

Дисертацијата е од областа на техничките науки

Посветено на моето семејство

Jugoslav Z. Achkoski, M.Sc.

Usage of Service-Oriented Architecture for Developing Prototype of Intelligence Information System

ABSTRACT: Trends in contemporary society influence on information systems development because benefits of their usage directly influence on achivments in society. Modern information technology considerably contributes to the processes' (activities) improvement by supporting intelligence cycles (planning, collecting data, analyzing data and dissemination). Although, there is constant improvement in the field of information technology, significant advancement in the quality of work in the field of intelligence has not taken place in the last ten years in Republic of Macedonia.

Usage of Service-oriented architecture (SOA) for designing distributed information system is the most advanced solution for information system development. The reason about this statement refers to the projects that are tightly related to development of service-oriented information system. In the same context, it can be highlighted solutions for creating distributed information systems based on SOA, where govermental actors are responsible for projects i.e Republic of Macedonia.

Conducted researches on usage of SOA indicate its implmentation in almost all spheres of society, where distributed information systems are needed. One of that spheres in society is National Security with Intelligence as a component of state security.

Research in this PhD thesis refers to usage of SOA for designing Intelligence Information Systems (IIS). Implementation of Service Oriented Architecture – SOA, i.e. the usage of SOA provides possibilities for making new opportunities in the form of expanded solutions for designing intelligence information systems, regarding the more efficient management of information, as well as their use by the end users for whom hum they are intended. Model of IIS that is proposed in this PhD thesis is based on Intelligence disciplines that are used as a foundation for integrated intelligence development.

Integrated Intelligence system allows information sharing between agencies, departments, institutions, sectors and other stakeholders involved in the process of intelligence, in order to create intelligence products that will improve decision-making process by the authorities.

In addition, particular attention must be paid on authentification and security of data and information that are treated.

Conducted researches and obtained results related to this PhD thesis showed excellent developed model of intelligence Information System that contributes in developing efficient model of Ingellignece that answer to requirements for intelligence cycle on which contemporary model of Intelligence should be based.

KEY WORDS:

Service-oriented architecture, Model of Intelligence Information System, Security standards, Metrics for service availability, service reliability and service response time, Intelligence

М-р. Југослав Ж. Ачкоски

Примена на сервисно ориентирана архитектура за развој на прототип на информациски систем за разузнавање

РЕЗИМЕ: Современите општествени трендови, влијаат на софистицираниот развој на информациски системи, бидејќи придобивките од нивното користење, влијаат на развојот на самото општество. Примената на современета информациска технологија во голема мера придонесува за подобрување на процесите (активностите) кои го поддржуваат разузнавачкиот циклус (планирање, собирање, анализа и десиминација). Иако постои константен напредок во ова поле, во последните десет години во Р. Македонија не се случила значајна разлика во квалитетот на работењето во областа на разузнавањето, предизвикано, од напредокот на информацискатa технологија.

Користењето на сервисно ориентираната архитектура за креирање на дистрибуирани информациски системи, претставува едно од најнапредните решенија за развој на ДКС. Причината за наведената констатација е во проектите за градба на информациски системи, кои секојдневно се развиваат, а се базираат на СОА. Во ист контекст, може да се нагласат и решенијата за креирање на дистрибуирани информациски системи базирани на СОА, за кои како носител во проектите е државата, односно Република Македонија.

Извршените истражувања за искористеноста на СОА, укажуваат на нејзина примена во скоро сите сфери на општеството, каде се појавува потреба од креирање на дистрибуирани информациски системи. Една од сферите е, и Националната безбедност, односно разузнавањето, кое ја претставува компонентата во системот за безбедност на државите.

Истражувањето во оваа докторската дисертација е насочено во креирање на модел на информациски систем за разузнавање со примена на сервисно ориентирана архитектура. Воведувањето на сервисно ориентираната архитектура во информациските системи, односно нејзина примена, овозможува создавање на нови можности за проширување на решенијата за дизајнирање на информациските системи за разузнавање во однос на поефикасно менаџирање со информациите. Креираниот модел на информациски систем, од аспект на разузнавањето, се базира на разузнавачките дисциплини, кои се искористени како основа за создавање на интегрирано разузнавање.

Системот за интегрирано разузнавање треба да овозможи размена на информациите помеѓу агенциите, службите, институциите, секторите и другите учесници вклучени во процесот на разузнавање, со цел

изработување разузнавачки продукти, преку кои ќе се овозможи правилно донесување одлуки од страна на авторитетите.
При тоа, особено внимание мора да се посвети на автетичноста и сигурноста на податоците и информациите кои се третираат.
Извршените истражувања, како и добиените резултати поврзани со темата, според актуелноста на третираната проблематика, методологија на истражувањето, содржината, како и очекуваните резултати, укажуваат дека развиениот модел на информациски систем за разузнавање претставува значаен придонес во развој на ефикасен модел за разузнавање, врз кој треба да се базира разузнавањето во Р. Македонија.

КЛУЧНИ ЗБОРОВИ: сервисно ориентирана архитектура, модел на информациски систем за разузнавање, сигурносни стандарди, метрики за расположливост на сервиси, веродостојност на сервиси, време на одговор на сервисите, разузнавање.

Докторската дисертација е изработена на Факултетот за информатички науки и компјутерско инженерство во Скопје, Р. Македонија. На менторот Вонр. проф. д-р Владимир Трајковиќ му должам огромна благодарност за континуираната искрена поддршка, сесрдно залагање, упорност, посветеност, корисните совети и за времето и вниманието кои ми ги посвети во текот на работата на докторската дисертација.

Искрена благодарност до сопругата Марија, синот Дамјан и ќерката Јана за бескрајната љубов, трпеливост и разбирање, несебичната поддршка и постојаната помош.

На крај, би сакал да ја изразам својата огромна благодарност и до моите родители Зора и Живко и мојот брат Далибор за бескрајната поддршка, помошта и љубовта пружени како во текот на работата на докторската дисертација, така и во животот.

СОДРЖИНА

ЛИСТА НА СЛИКИ

ЛИСТА НА ТАБЕЛИ

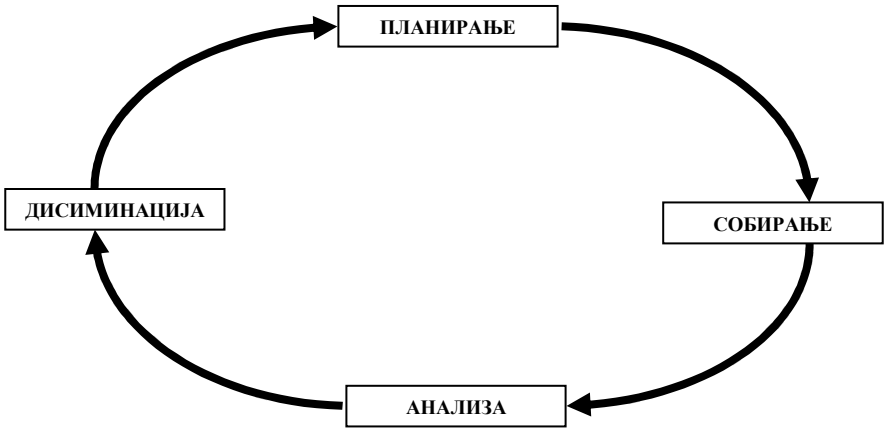
ГЛАВА 1

ВОВЕД

1.1 Мотивација за изработка на докторската дисертација

Разузнавањето, како сервис, е од витално значење за една држава ([1], [2]). Информациските системи за поддршка на разузнавачките активности се секојдневие и нивното искористување има големо влијание во процесот на донесување на одлука од авторитетите во разузнавањето. Примената на современета информациска технологија во голема мера придонесува за подобрување на процесите (активности) кои го поддржуваат разузнавачкиот циклус (планирање, собирање, анализа и десиминација). Иако постои константен напредок во ова поле, значајна разлика во квалитетот на работењето во областа на разузнавањето, предизвикана од напредокот на информацискатa технологија, не се случило, во последните десет години ([3], [4], [5]).

Операциите или фазите прикажани на Слика 1 кои се дефинирани согласно „NATO Glossary of Terms and Definitions (AAP-6)“ ([105]) се:



Слика 1. Разузнавачки циклус

1) *Планирање*
   “Одредување на приоритетни разузнавачки побарувања, планирање на разузнавачки операции за собирање на податоци, врз основа на побарувањата на агенциите или разузнавачките служби”

2) *Собирање:*
   “Експлоатација на изворите од страна на агенциите и доставување на информациите до соодветни единици за обработка, овластени за нивно користење во изработката на разузнавачки продукти.”

3) *Анализа*:

"Изработка на разузнавачки продукти преку составување, евалуација, анализа, интеграција и интепретација на информациите, како и користење на други методи за изработка на разузнавачки продукт."

4) *Дисиминација*:
"Навремено доставување на разузнавачки продукти во форма за користење од страна на крајните корисници за кои тоа е потребно."

Воведувањето на сервисно ориентираната архитектура (или кратко: СОА) во информациските системи ([6]), односно нејзина примена, овозможува создавање на нови можности во форма на проширување на решенијата за дизајнирање на информациските системи за разузнавање ([7], [8], [9], [10], [11]) во однос на поефикасно менаџирање со информациите, како и нивно искористување од крајните корисници за кои истите се наменети. Заради одржување на чекорот со современите развојни трендови, потребно е краткорочно, среднорочно и долгорочно планирање на ресурси за развој на информациски системи за поддршка на разузнавањето ([12], [13], [14]) во однос на развојот на информацискатa технологија.

Имплементацијата на сервисно ориентирана архитектура ([15], [16]) во информациските системи ([17]) е логично решение, кое не е само привремено и за краткорочни цели, туку перспективно решение за целокупната стратегија на институциите и компаниите.

Секој современ разузнавачки сервис е базиран на информациски систем ([18], [19], [20], [21]). Примената на високи технологии, особено на информациско-телекомуникацискатa технологија (ICT), овозможува поефикасно извршување на функциите на разузнавањето, во однос на собирање, планирање, анализирање и десиминацијата на податоци ([22], [23], [24], [25]).

Главната цел на оваа докторска дисертација ќе биде примена на сервисно ориентирана архитектура во прототип на информациски систем за разузнавање (ИСР). Како едно од можните решенија е СОА како основа за создавање на употребливи сервиси [26] кои ќе бидат составни компоненти на информацискиот систем за разузнавање.

Традиционалниот разузнавачки циклус е процес со прецизно дефинирани чекори во кој различни сектори имаат строго дефинирани функции, фокусирани на извршување на задачи од нивниот делокруг на работа во корелација со наведениот процес, додека другите аспекти од разузнавачкиот циклус се препуштаат на други сектори или единици на кои им се доделени други функции и надлежности. Наведениот пристап се третира како несоодветен во „network-centric" операциите (операции со комплексни, динамични и нелинеарни мрежи, кои во моментот претставуваат најголем предизвик за разузнавачката заедница во информацискатa ера). Во денешницата, како одговор на предизвикот, современите разузнавачки агенции имаат воспоставено тимови за следење и одговор на настани на различни локации, употребувајќи современи информациско-комуникациски решенија за подобра координација.

Од друга страна, современиот „target-centric" моделот на разузнавање, особено процесот на анализа, не претставува нов концепт на модел на разузнавање, но истиот не е официјално прифатен од разузнавачката заедница.

Поединци и мали тимови создаваат „ad-hoc" бази на податоци за креирање на релеватни информации, сè со цел подобрување на процесот на анализа на информациите. Сепак, повремено креираните бази на податоци се несоодветно решение за разузнавачката

заедница, бидејќи не можат да одговорат на потребите на аналитичарите на информациите. Базите на податоци кои содржат информации се најчесто неразбирливи за аутсајдерите. Смената на моделите на разузнавањето, односно преминувањето од традиционално во модел на „target-centric“ разузнавање, им овозможи на аналитичарите на информации, како дел од разузнавачката заедница, да ги искажат своите барањата и потреби од воведување на нови информациско-комуникациски технологии и следење на нивниот развој при користење, сè со една и единствена цел – креирање на подобри разузнавачки продукти.

Во докторската дисертација ќе се направи обид да се постигнат следните цели:

1. Истражување на значењето на сервисно-ориентираната архитектура за изградба на дистрибуираните информациски системи за потребите на разузнавањето;
2. Компаративна анализа со други модели на информациски системи за разузнавање, согласно јавно достапните описи;
3. Развој на модел на информациски систем за разузнавање, кој овозможува задоволување на дисцплините (IMINT, SIGNT, MASINT, ELINT, OSINT, HUMINT), како и разузнавачкиот циклус на кои се базира разузнавањето во Р. Македонија;
4. Анализа и селекција на информациски системи од проектот „e-Gov“ (2004 – 2011 год.) на Р. Македонија, базирани на сервисно-ориентиранаархитектура, потребни за интеграција со информацискиот систем за разузнавање (ИСР);
5. Развој на модел, начин и метод за интеграција на апликациите на селектираните информациски системи со ИСР за потребите на разузнавањето во Р. Македонија;
6. Истражување на можностите за искористување на соодветни стандарди (посебно сигурносни) со цел надминување на предизвиците од зависноста на информациските системи од еднообразната технологијата и воспоставување на информациски систем базиран сервисно-ориентираната архитектура во целост;
7. Дефинирање на метрики за евалуирање на сервисите во сервисно ориентиран систем и евалуирање на сервисите во информациски систем за разузнавање базиран на СОА.

1.2 Преглед на досегашните истражувања во оваа област

Во рамките на проектот ([27]) „e-Gov“ на Република Македонија, кој е започнат 2004 година со рок на имплементација до 2011 година, развивани се решенија кои треба да ја зголемат ефикасноста и транспарентноста на јавниот сектор, како и водење на бизнис на сигурен начин, заради следење на современите трендови и создавајќи модерно општество.

Во рамките на проектот развивани се апликации, кои имаат за цел да воспостават интеракција помеѓу владините институции и бизнис заедницата (*engl.*Goverment to Business (G2B)), државната администрација и граѓаните (*engl.*Goverment to Citizen (G2C)) или интеракција помеѓу владините институции (*engl.*Goverment to Govermnt (G2G)).

Информациски системи кои се препознаени во рамките на проектот за потребите на ИСР се информацискиот систем „Documentum“, информацискиот систем „eParliament“, информацискиот систем „IBMS“ и информацискиот систем „Interoperability System“.

Наведените системи се базирани на сервисно орентираната архитектура, при што поврзувањето ([28], [29], [30], [31]) на ИСР со наведените информацини системи се поедноставува.

Информацискиот систем „Documentum“ е наменет за менаџирање и складирање на документи со разнолики функционалности и истиот преставува платформа за поврзување со останатите системи и апликации на институциите во РМ. Платформата на „Documentum“ системот е лесна за надоградување во однос на потребите на корисниците и преставува основа за изведба на работните процеси и интеграција со комплексни апликации кои имаат задача да го автоматизираат процесот на анализа и процесирање на информациите.

Како корисници на системот и начелната интеракција која се воспоставува во спецификацијата, се наведуваат Влада на РМ, Министерства, Генерален секретаријат, Собрание на РМ, Секретаријат за правда, Секретаријат за Евро-атлански интеграции, Секретаријат за имлементација на Охридски рамковен договор, Служба за административни работи.

Информацискиот систем „eParliament“ се однесува за внатрешни правни процеси, подготовките и одржувањето на седниците, обезбедувајќи високо ниво на ефективност, намалување на трошоците, мобилност, транспарентност и одговорност во процесот на подготовка, имплеметација и дневна координација во одлуките произлезени од правниот процес од Собранието на Република Македонија. Во исто време, системот ги интегрира Собранието на РМ и различни институции и ги процесира во дистрибуирани и оркестрирани процеси кои го трансформираат правниот процес од хартиен во без хартиен процес.

Како корисници на информацискиот систем eParliament, освен оние за кого е директно наменет, се појавуваат следните: членови на Собрание на РМ, население, институции (Влада, министерства и агенции и други владини тела, комисии и државни органи).

Интегриран систем за гранично управување – „IBMS“ обезбедува платформа за размена на информации, за контрола и надгледување на границата. Системот користи база на податоци за управување со границата при што се обезбедува координиран пристап до информации помеѓу државните органи, кои имаат надлежност во граничното управување.

Како корисници на наведениот систем се појавуваат компании/патници, Центар за интегрирано гранично управување (ИГУ), МВР и други институции и гранични пунктови.

Информацискиот систем „Interoperability System“ е наменет за побрза и поефикасна размена на податоци меѓу државните институции, при што со нивната поврзаност во системот за интероперабилност се избегнува дуплирање на податоците и правање грешки, а институциите остануваат поефективни.

Исто така, со системот треба да се оствари интерконекција на регистрите и базите на податоци меѓу државните органи и институции, во напредната фаза од проектот „e-Gov“ (2004 -2011 год.).

Во пилот фазата на проектот, при развој на системот опфатени се следните корисници: Царинската управа, МВР, Централниот регистар, Управата за јавни приходи и катастарот.

Според консултираната достапна литература, добиени се сознанија дека во голем број на технолошки напредни држави, освен имплементација во цивилниот домен,

примената на сервисно-ориентираната архитектура во воениот домен е приоритет на авторитетите, со една единствена цел - зголемување на безбедноста во општеството. Од таа причина, како и врз основа на прилагодувањето на општеството на продорноста на технологијата и искористување на бенифитите од истата, развивани се бројни истражувачки проекти како составни компоненти на владини развојни програми.

Во ([32]), трудот со наслов "Extending Service Orientated Architectures to the Deployed Land Environment", укажува дека интересот за сервисно-ориентираната архитектура води кон зголемено користење на СОА во информациско комуникациските системи во воениот и цивилниот домен. Колку што е поедноставно имплементирањето на СОА ([33], [34], [35], [36]) базирана на функционалност во непроменлива организациска инфраструктура, поедначкво исто толку има фактори кои го компликуваат имплементирањето на СОА во дизајн на системи за воени цели. Имплементирањето на сервисно-ориентиранаархитектура во системите на распоредените копнени единици во мисија кои извршуваат борбени операции или друг вид на мисии (како што се на пример мисии за воспоставување на мирот или негово одржување водени од НАТО, ЕУ или ООН) преставува предизвик за ефективна имплементација на СОА во воениот домен.

Во ([37]), трудот со наслов "Service Benefits – Life Beyond SOA" користењето на сервисно ориентираната архитектура во креирање на системите, овозможува реорганизирање на бизнис процесите ([38], [39], [40]) и нивна оптиматизација, дозволувајќи користење и имплементирање на апликации независно од платформата, како и интегрирање на истите во организациската инфраструктура. Примената на сервисно ориентираната архитектура нуди и бенифит во однос на достапност на сервисите за интеракција со надворешните партнери, на пример нејзината примена во ланецот за набавка со партнерите и останатите учесници ([41], [42], [43]). Новите генерации на апликации со интегрирацијата на процесите на автоматизација, интегрирањето на информациите и бизнис анализа им дозволуваат на операторите да ги зголемат и прошират бенифитите од користењето на сервисно-ориентираната архитектура. Исто така, досегашните истражувањата кои се однесуваат на наведената проблематика укажуваат дека се креирани бројни информациски системи со тежиште на еволуција на бизнис процесите и информациите кон сервисно-ориентираната архитектура и дизајнирано решенија кои овозможуваат решенија за критични мисии и за централно координарини воени операции (*engl.* network centric operations).

Во ([44]), трудот со наслов "Introducing the Triton SOA Foundation for Military Systems Integrators and Developers" за дефинирањето на идните архитектури, се тврди дека авторитети задолжени за дефинирање на безбедносниот систем ја имаат препознато потребата за креирање на генерална или потполна сервисна платформа која би се користела за оперативните воени апликации и сервиси. Како примери се наведуваат концептите за „Network Core Services" на Американското министерство за Одбрана (*engl.* Department of Defense (DoD)) и „Network enabled core services" на НАТО. Во ист контекст, и Австралиското министерство за одбрана има предложено слична архитектура (Single Information Environment Architectural Intent 2010). Имплементирањето на сервисната платформа е овозможено со користење на „COTS" технологии. На тој начин е создаден „IBM SOA Foundation (Triton Core)". „Triton" е интегриран, сет од „COTS" софтверски продукти, практичен и составен од шеми кои обезбедуваат елементи кои се потребни за имплемтирање на СОА ([45], [46], [47]) за интегрирање во организациските постоечки инфраструктури [48], без финансиски импликации за кодирање и модифицирање.

Системот „Triton Core“ се состои од „Enterprise Service Bus (ESB)“ и јадро на сервиси ([49], [50], [51], [52], [53], [54]) кои ги поврзуваат останатите сервиси ([55], [55], [56]), апликации и ресурси, сè со цел да се воспостави “Net-Centric” решението. Со креирањето на системот „Triton Core“ се намалени трошоците во Австралиското министерство за одбрана, како и во одбранбената индустрија на Австралија во целост, а исто е зголемена и ефикасноста од примената на пристапот кон „Single Information Environment“ архитектура.

Во ([57]), трудот со наслов “Finnish Defense Forces – Network-Centric Operations“, Финското министерство за одбрана, како и сите останати организации кои се справуваат со кризите и конфликтите, како што се Ураганот Катрина, епидемијата „SARS“ или придонесот со воени единици во Ирак, Авганистан, Балканот и други локации, бараат да го зголемат учеството во коалицијата со различни специфики на воените и цивилните организации. Критичните сценарија кои може да се очекуваат се координација помеѓу военото воздухопловство, морнарицата, полицијата, болници и други установи за јавно здравство, и други воени и цивилни групи за инволвираните групи да бидат ефективни во извршувањето на оперативните активности во таква околина, мора брзо да реагираат и да се прилагодат на интеграцијата во дејствувањето, со цел да се избегнат стресните и непридвидените ситуации. Технолошката некомпатабилност може да ја комплицира координацијата, во моментот кога групите користат различни технички архитектури и комуникациски протоколи. Како пример за некомпактабилноста може да се наведат нападите во САД на 11-ти Септември, каде полицијата и секторот за спречување на пожари не биле во можност да комуницираат бидејќи нивните радио системи биле некомпатибилни. Последица од некомпатибилноста е нефункципонирање на системот за предупредување. На истиот начин и Финското министерство за одбрана се базирало на “silo-ed” технологијата, при што функционирањето на системот во итни ситуации било несоодветно. „C4 (command, control, communications and computing)“ системите биле креирани за подршка на воениот домен, но сепак овие системи се „stove-piped“ за да ги поддржат копнените единици, морнарицата и операциите на военото воздухопловсто. Врз основа на наведената причина, не е дозволен развој на идните системи врз старите системи и надминување на недостатоците од застарената технологија. Развојот на идните системи е замислен да се изврши со интеграција ([48]) на технологијата, податоците и апликации. Заради остварување на целта развиена е програма „FiNED“ за имплементирање на сервисно ориентираната архитектура, со една единствена цел – зголемување на ефикасноста и креирање на повторно употреблива технологија ([58], [59], [60], [61], [62]). Одредено е користење на „COTS“ пакетите како што се „Oracle“, „SAP“, „Tivoli“ и „Lotus Notes“ од економски аспект, бидејќи дополнителни финасисиски импликаци се непотребни. Предвидено е новата архитектура на Финското министерство за одбрана да се базира на потполна сервисна платформа ([63], [64], [65], [66], [67], [68], [69], [70]) вклучувајќи ги сите области од воениот домен. Специфичните функции според програмата „FiNED“, предвидено е да бидат на највисокото ниво на платформата.

Во ([71]) трудот со наслов “Supporting Capability Evolution Using a Service Oriented Architecture Approach in a Military Command and Control Information System“ е објаснето дека информациските системи за командување и контрола (К2) во штабовите на оперативно ниво се базирани на СОА. Со цел да се зголеми можноста за размената на информации во воените средини, СОА пристапот дозволува флексибилно зголемување на

можноста за размена на информациите преку интеграција и интероперабилност на системите базирано на „commercial-off-the shelf technology (COTS)“ и стандарди.

1.3 Придобивки од докторската дисертација

Најзначајна придобивка од докторска дисертација е примена на сервисно ориентирана архитектура во развој на модел на информациски систем за разузнавање, кој овозможува задоволување на дисцплините на разузнавање (IMINT, SIGNT, MASINT, ELINT, OSINT, HUMINT), како и разузнавачкиот циклус на кои се базира разузнавањето во Република Македонија. При тоа посебно е акцентирана примената на СОА, како основа за создавање на нови, употребливи сервиси кои ќе бидат составни компоненти на информацискиот систем за разузнавање. Развиениот модел е илустриран со прототип кој ќе треба да послужи за истражување на значењето на сервисно ориентираната архитектура за изградба на дистрибуираните информациски системи за потребите на разузнавањето.

Развиениот моделот на ИСР е евалуиран преку компаративна анализа со други модели на информациски системи за разузнавање за што се користени информации согласно јавно достапните описи.

Од извршените истражувања и разработената тематика поврзана со докторска дисертација, направена е сублимација на најважните придобивки:

1. Дефиниран модел на информациски систем за разузнавање кој овозможува задоволување на дисцплините (IMINT, SIGNT, MASINT, ELINT, OSINT, HUMINT), како и разузнавачкиот циклус на кои се базира разузнавањето;

2. Дефиниран модел, начин и метод за интеграција на апликациите на селектираните информациски системи со ИСР за потребите на разузнавањето во Р. Македонија;

3. Дефинирање и опис на соодветни стандарди со цел надминување на предизвиците од зависноста на информациските системи од еднообразната технологијата и воспоставување на информациски систем базиран во целост на сервисно ориентираната архитектура;

4. Селекција и опис на безбедносни стандарди кои треба да се користат во ИСР, со цел контролиран пристап до информациите и евиденција на корисниците;

5. Дефинирање на протокол за дистрибуирано пребарување на информации од временски лимитиран карактер во зависност од итноста (online или near-line), со цел правовремено донесување на одлуки од страна на авторитетите;

6. Прототип портал и опис и имплементација на соодветни модули, со цел задоволување на дисциплините на разузнавањето;

7. Развој на прототип сервиси базирани на разузнавачките дисциплини и нивно користење во создавање на разузнавачки продукти;

8. Дефинирани се генерални метрики кои се употребени за евалуирање на сервисите во сервисно ориентиран систем и специјални метрики кои искористени за евалуирање на сервисите во информациски систем за разузнавање базиран на СОА.

Со ИСР ќе се даде придонес во јакнењето на безбедноста преку собирањето на податоци и нивно вметнување во информациските системи, селекција на информациите, односно создавање на информации од необработени податоци, потоа искористување на податоците и изработка на разузнавачки продукти и десиминација на истите до авторитетите за донесување на соодветна одлука и превземање на соодветна акција.

1.4 Структура на докторската дисертација

Во **втората** глава на оваа докторска дисертација се истражувани функционалностите на крајните корисници на ИСР. Корисничките функционалности на системот за разузнавање можат да се третираат од повеќе аспекти, согласно со поделбата на корисници. Разузнавањето, како еден од корисниците се базира на четирите разузнавачки дисциплини: „IMINT“, „SIGINT“, „MASINT“ и „OSINT“. Исто така, дисциплините се разделуваат на поддисциплини со различни специфики во делокругот на работата и може организационо да припаѓаат на повеќе институции или единици во состав на Одбранбените сили на државата (Агенција за разузнавање (АР), Министерство за внатрешни работи, Министерство за одбрана, Министерство за Здравство, Министерство за надворешни работи и други субјекти), но нивната улога и задача е да внесуваат податоци (информации, проценки, анализи, извештаи и др.), прават нивна верификација (што може да биде предмет на поддршка на ИСР) и добиваат нотификации или налози (на пример за политичко-безбедносната состојба во одредена држава во однос на сигурноста на инвестицијата). Оваа поглавје резултира со предлог модел на ИСР.

Во **третата** глава е извршено истражување на јавно достапните решенија за информациски системи кои се во функција на разузнавањето. Во поглавјето е истражувано значењето на СОА за изградба на информациските системи. Исто така, направена е анализа на придобивките од користењето на СОА при дефинирањето на модел на ИСР, со цел да се потврди дека е избрана вистинската технологија. Тежиштето во поглавјето е насочено спрема разработувањето на логичката и нивовската архитектура на ИСР.

Во **четвртата** глава е истражувана информациската инфраструктурата потребна за поддршка при размена на информации, при што истата мора да биде прилагодлива и да постои можност за нејзино проширување, за да се овозможи задоволување на идните потреби. Размената, односно користењето на информациите и нивната достапност на различни учесници во зависност од сигурносните полиси на информациските системи, во значителна мера ќе им помогне на авторитетите во процесот на донесување на одлуки, со што на полесен начин ќе ги планираат идните чекори. За да се оствари претходно наведеното, како крајна цел е дефиниран специфичен модел на интеграција на посточките информациските системи кој може да се користи со различни технологии и на различни интеграциски платформи.

Во **петтата** глава се истражуваат сигурносните стандарди потребни за задоволување на безбедноста за системот што е моделиран во докторската дисертација. Сигурноста на информациските системи базирани на СОА е разработена преку дефинирање на механизми (протоколи) и нови апликативни алгоритми кои што го штитат

системот од ненамерна или намерна штета. При дизајнирањето на моделот на ИСР, во поглавјето се креирани два тека (контролен и податочен тек), преку кои се разгледуваат предложените можни решенија за сигурност на системот. Разработениот модел на сигурност на ИСР е во согласност со моментално развиените станандарди за сигурност, кои се однесуваат на сервисно ориентираната архитектура.

Во **шестата** глава е опишан модел на информациски систем за разузнавање базиран на сервисно ориентирана архитектура, при што тежиштето е насочено во креирање метриките кои се однесуваат на опишаниот модел на информациски систем за разузнавање. Придонесот во поглавјето е презентиран преку развој на метрики кои ќе овозможат евалуирање на селектирани атрибути на сервисите. Во ист контекст разработени се метрики за евалуирање на *достапноста* на разузнавачката информацијата до определен сервис, проценка на *веродостојноста* на информација, како и проценка на *чинењето* на информациската аквизиција.

Во **седмата** глава се дефинирани метрики за расположливост на сервисите, веродостојност и време на одзив на сервисите, кои се потребни за презентирање на карактеристките на сервисите. „Quality of service (QoS)“ претставува карактеристика на сервисите преку која се утврдуваат одредени параметри на сервисите [110]. Без разлика дали станува збор за веб сервиси или сервиси кои се дел од одреден информациски систем, параметрите за „QoS“ играат значајна улога. Параметрите за „QoS“ создаваат кај корисниците доверба и сигурност за користење на сервисите. Корисниците на сервисите посакуваат користење на сервиси кои искуствено функционирале без проблеми, како на пример кратко време на чекање, висока веродостојност и можност за успешно користење на сервисите. „QoS“ пошироко може да биде категоризиран во три категории: перформанси, зависност и безбедност.

Во поглавјето се разработени параметри кои спаѓаат во првите две категории. Од првата категорија за параметрите на перформансите се разработува времето за одзив на сервисите, а за втората категорија за параметрите на зависност се разработени расположливост на сервисот (*engl.*availability) и веродостојност (*engl.* reliability).

Креираната метрика за одредување на просечното време за одзив на сервисите од кои е составен информацискиот систем за разузнавање, после креирано барање од корисниците за одредена информација, е потребна заради осетливоста на функциите и задачите кои се извршуваат во разузнавањето, а се од временски лимитиран карактер. Исто така, во поглавјето се креирани метрики за раположливост на сервисите (*engl.* service availability) во однос на нивната искористливост за крајните корисници и креирани се метрики за проценување на веродостојноста на сервисите (*engl.* service reliability assessment) на кои се базира информацискиот систем.

Исто така во поглавјето се разработени состојбите на сервисно ориентираниот информациски систем за разузнавање со користење на Маркови вериги.

Во последната (**осма**) глава се дадени заклучоците до кои е дојдено врз основа на анализите, имплементацијата и разработените метрики за евалуација на сервисите во сервисно-ориентираниот информациски систем за разузнавање.

1.5 Листа на објавени трудови поврзани со докторската дисертација

Трудови во меѓународни списанија:

[A1] **Jugoslav Achkoski**, Vladimir Trajkovik and Metodija Dojchinovski, "An Intelligence Information System based on Service-Oriented Architecture: A Survey of Security Issues," Information & Security: An International Journal, vol. 27 pp: 91-111. (2011)

[A2] **Jugoslav Achkoski**, Vladimir Trajkovik and Nevena Serafimova, "Metrics in Intelligence Information System Based on Service – Oriented Architecture (SOA)" Computer Science and Information Systems Journal, 2012 (*In Review*)

[A3] **Jugoslav Achkoski** and Vladimir Trajkovik, "Usage of Service-Oriented Architecture for Developing Prototype of Intelligence Information System" TEM Journal, 2012 (*Accepted*)

Трудови на конференции со зборник уреден од меѓународна издавачка куќа:

[A4] **Jugoslav Ackoski**, Vladimir Trajkovik, Metrics for Service Availability and Service Reliability in Service-oriented Intelligence Information System, International Conference ICT Innovations 2012, Skopje, Macedonia, September 12 – 15, 2012

[A5] **Jugoslav Ackoski**, Vladimir Trajkovik and Danco Davcev, Service-Oriented Architecture Concept for Intelligence Information System Development, The Third International Conferences on Advanced Service Computing SERVICE COMPUTATION 2011 (IARIA), Rome, Italy, September 25 - 30, 2011

[A6] **Jugoslav Ackoski**, Vladimir Trajkovik, Intelligence Information System (IIS) with SOA-based Information Systems, 33rd International Conference on INFORMATION TECHNOLOGY INTERFACES, IEEE, Cavtat/Dubrovnik, Croatia, June 27 - 30, 2011

[A7] **Jugoslav Ackoski**, Vladimir Trajkovik and Danco Davcev, Security Issues for Intelligence Information System based on Service-Oriented Architecture, International Conference ICT Innovations 2011, Skopje, Macedonia, September 14 – 16, 2011

[A8] **Jugoslav Ackoski**, Vladimir Trajkovik and Metodija Dojcinovski, SOA Approach in Prototype of Intelligence Information System, International Conference ICT Innovations 2010, Ohrid, Macedonia, September 2010

Останато:

[A9] Славко Ангелевски, **Југослав Ачкоски**, Невена Серафимова, Концепт за моделирање и симулации во справување со кризни ситуации,ЕТАИ, Охрид, Р. Македонија, Септември 2009 година.

[A10] **Југослав Ачкоски**, Славко Ангелевски, Димитар Богатинов, Прототип апликација за Е- Архив**,** ЕТАИ, Охрид, Р. Македонија, Септември 2009 година

[A11] **Југослав Ачкоски**, Методија Дојчиновски, Сајбер криминал и заштита на дигиталните податоци во компјутерските мрежи, Национално теоретско списание „Современа македонска одбрана“, Скопје, Р. Македонија, Април 2011

[A12] **Jugoslav Ackoski**, Vladimir Trajkovik, Intelligence Information System Integration, The 8th International Conference for Informatics and Information Technology (CIIT 2011), Bitola, Macedonia, March 2011

[A13] Metodija Dojcinovski, **Jugoslav Ackoski,** Application of Contemporary Intelligence Models in Terms of Transformation and Security Sector Reform, International Conference Security in the Post-Conflict (Western) Balkans: Transition and Challenges Faced by the Republic of Macedonia (Security Studies and the Science of Security), Ohrid, Macedonia, May 27 - 28, 2011

[A14] Мухамед Ибраими, **Југослав Ачкоски**, „Современи трендови на разузнавањето во борба против тероризмот“. Зборник на трудови од Научно-стручна конференција „MILCON ’12“, Скопје, Р. Македонија, стр. 159 – 165, 14.05.2012

[A15] Зоран Стојановски, Методија Дојчиновски, **Југослав Ачкоски**, „Сајбер тероризмот - закана за системите за поддршка на процесот на планирање на современите операции“. Зборник на трудови од Научно-стручна конференција „MILCON ’12“, Скопје, Р. Македонија, стр. 225 – 230, 14.05.2012

[A16] **Jugoslav Ackoski** and Metodija Dojcinovski, Cyber Terrorism and Cyber Crime – Threats for Cyber Security, In Proceedings of First Annual International Scientific Conference Organized by “MIT University – Skopje”, Makedonski Brod, Macedonia, June 09, 2012

ГЛАВА 2

КОНЦЕПТ ЗА РАЗВОЈ НА ИНФОРМАЦИСКИ СИСТЕМ ЗА РАЗУЗНАВАЊЕ БАЗИРАН НА СЕРВИСНО ОРИЕНТИРАНА АРХИТЕКТУРА

Ова поглавје е разработено во 3 (три) секции. Во првата секција е опишан модел на информациски систем за разузнавање. Во втората секција се разработуваат функциите на дистрибуираниот ИСР. Во третата секција се презентирани очекуваните резултати кои треба да бидат добиени со имплементацијата на СОА концептот за развој на информациски систем за разузнавање.

2.1 Модел на информациски систем за разузнавање

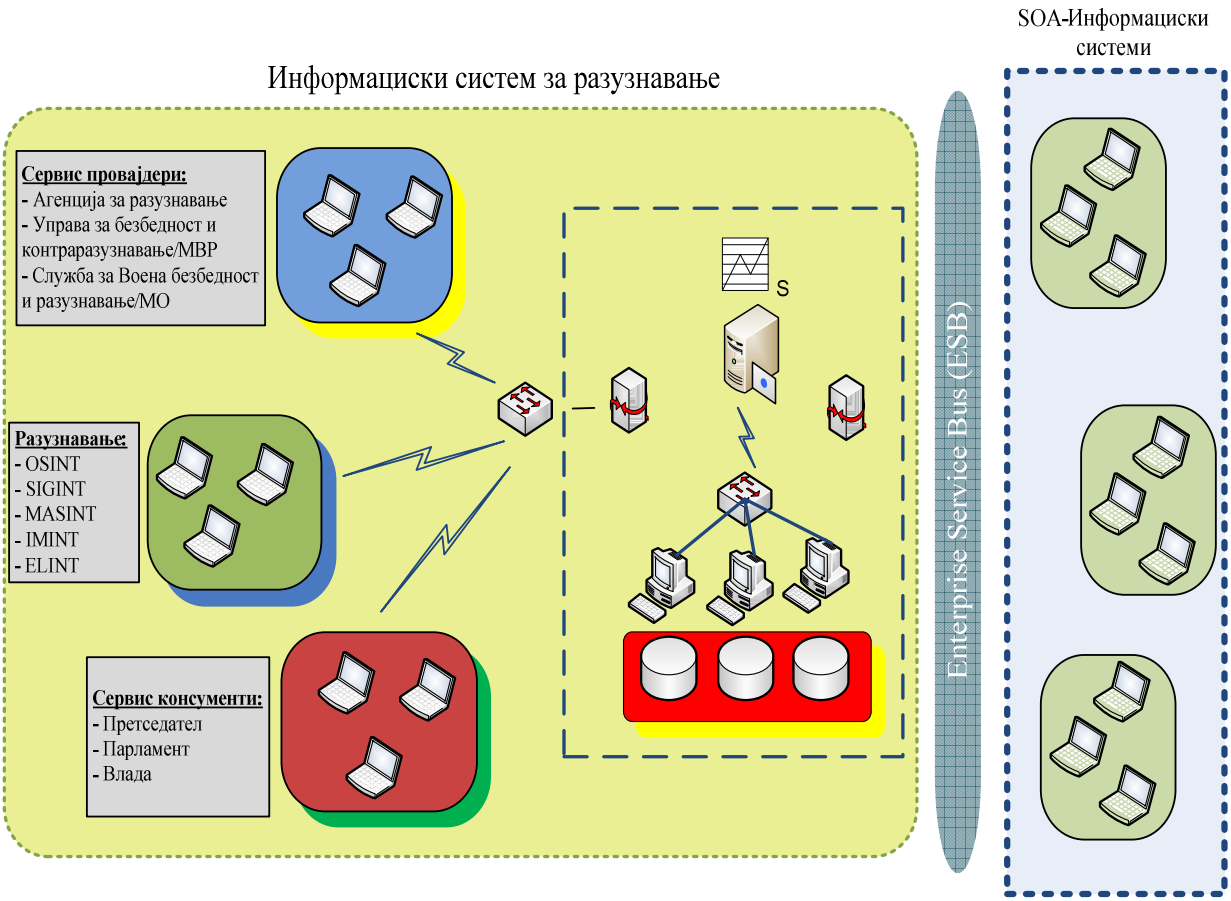
Моделот на СОА базиран информациски систем за разузнавање прикажан на Слика 2, би требало да ги исполни функциите и задачите на разузнавањето кои произлегуваат од поставени комплексни барањата, а исто така моделот треба да овозможи интеграција со информациските системи на другите институции кои имаат улога во разузнавањето.

Презентираниот модел на ИСР содржи три типа на корисници: сервис провајдери, корисници на сервиси(сервис конзументи) и разузнавање. Корисниците на сервисите се институциите (Центар за кризен менаџмент(ЦУК), МВР, Агенција за разузнавање или други), кои имаат потреба да користат информации од ИСР или да доставуваат информации заради предупредување или известување.

Врз основа на воспоставените безбедносните процедури, сервис провајдерите обезбедуваат информации за корисниците на сервисите.

Разузнавањето како трет тип на корисник во ИСР, како што е претходно напоменато, се базира на повеќе разузнавачки дисциплини „IMINT“, „SIGINT“, „MASINT“, „OSINT“ итн. Со цел да се одговори на барањата на разузнавачките дисциплини, потребно е да се исполнат повеќе задачи и тоа: собирање на информации (проценки, анализи, креирање на извештаи итн.), нивна верификација и дисиминација (*пример:* проценка за политичката и безбедносната ситуација во странска земја во однос на сигурноста на инвестициите.)

Сите сервиси добиваат информации од адекватни сервис провајдери, како информациските системи на владините институции или агенции кои се вклучени во разузнавачкиот циклус. Исто така, постои можност други информациски системи да бидат сервис провајдери за интер-институциска размена на информации. Сервис провајдерите со помош на системите за поддршка на работните процеси, дефинираат веб сервиси кои се користат од корисниците, врз основа на соодветно безбедносно ниво во сервисниот регистер.



Слика 2. Модел на информациски систем за разузнавање базиран на СОА

Методологијата за развој на СОА базиран информациски систем за разузнавање се основа на неколку постулати. Искуствата од неодамнешните истражувања, кои се однесуваат на употребата на СОА во дизајнирање на информациски системи, покажуваат дека агенциите, секторите, институциите и другите учесници можат ги вметнуваат и повлекуваат податоци на флексибилен и стандардизиран начин преку комуникациски интерфејс со користење на веб сервиси и „XML schema“.

Првиот постулат ја дефинира методологијата за размена на податоци во сервисно ориентирана околина. Методологијата за размена на податоците треба да го задоволи условот кој се однесува на јавно опишаните достапни решенија за информациски системи кои ги поддржуваат разузнавачките функции.

Вториот постулат треба да се фокусира за употребата на СОА во дизајнирање на информациски системи, со интенција за наоѓање на оправданост за развој на инфомациски систем за разузнавање. СОА треба да се третира како стандард за повторна употреба на податоците, кое се овозможува преку „loosely coupled“ (лабави врски, односно сервисите или апликациите може да се преобликуваат на најпогоден начин за корисниците, а со самото тоа и информациските системи). Постулатот овозможува независност од имплементацискатa платформа, овозможувајќи измена на хардверот и софтверот без негативни импликации на другите компоненти од информацискиот систем, сè додека комуникацискиот интерфејс на сервисот не се измени.

Третиот постулат ги опишува функционалностите на системските крајни корисници. Врз основа на поделбата на корисниците, функционалностите на корисниците може да бидат истражувани од различни аспекти. Разузнавањето како краен корисник во ИСР, е базирано на разузнавачки дисциплини кои се поделени на разузнавачки поддисциплини. Наведените дисциплини се имплементираат различно како сервиси во рамките на владините институции, секторите или воените борбени единици како составни компоненти од националниот безбедносен систем (Агенција за разузнавање, Министерство за внатрешни работи (МВР), Министерство за одбрана (МО), Министерство за надворешни работи (МНР) и други). Разузнавачките сервиси може да се поделат во три категории: сервиси за внесување на податоци, сервиси за верификација на податоците и сервиси за нотификација (проценка на сервисите за одредена разузнавачка служба може да се разликуваат во зависност од безбедносните политики на државата)

Четвртиот постулат разработува концепт за развој на ИСР согласно барањата кои се очекуваат во иднина. Со цел да се задоволат идните барања, информацискатa инфраструктура би требало да биде флексибилна и лесно адаптивна, бидејќи е потребно потполна поддршка за воспоставување на процес за размена на информации помеѓу учесниците. Размената на информациите би требало да биде основа за развој на системот. Тоа може да им помогне на авторитите во процесот на донесување на одлуки, овозможувајќи им да ги планираат акциите на соодветен начин. Со цел да се постигне претходно наведеното, потребно е дефинирање на модел на информациски систем каде што интеграцијата со останатите системи ќе биде овозможена независно од моменталната технологијата и интеграцискатa платформа.

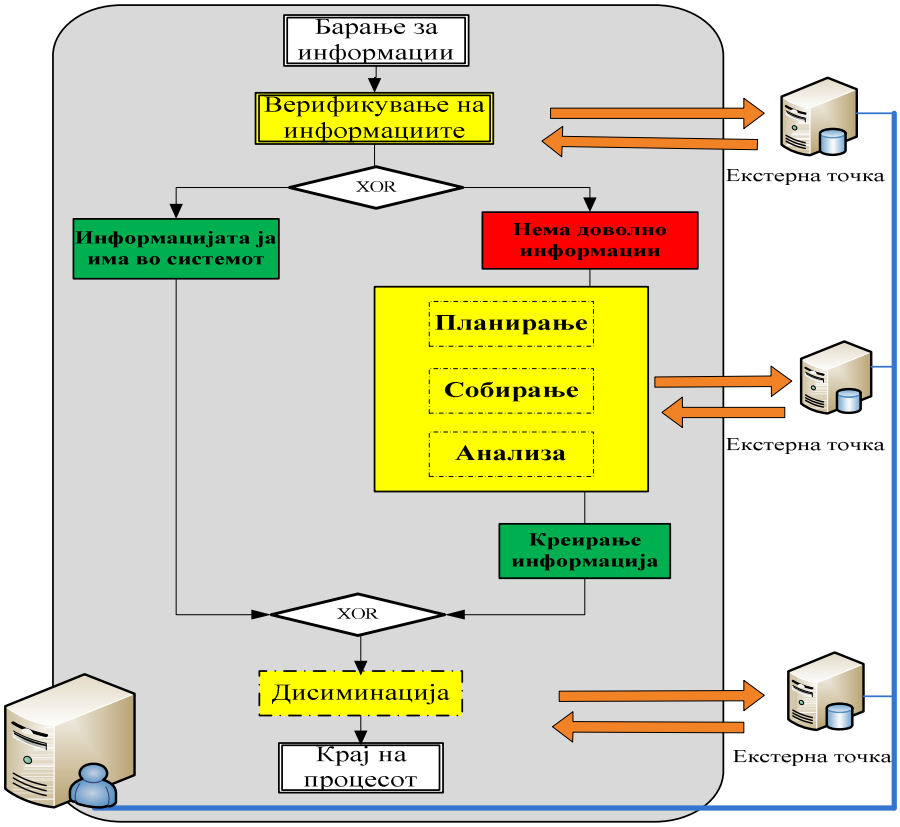
Со петтиот постулат се опфатени безбедносните стандарди на информацискиот систем кои е потребно да се имплементираат, со цел да се постигни одредене ниво на безбедност. Сервисно-ориентираните информациски системи треба да бидат заштитени од навлегување во ситемите и други видови на сигурносни пропусти и закани. Терминот „сигурност“ во вакви околности индицира на воспоставување на механизми наменети за заштита на функциите на системот. Во фаза на дизајнирање на системот, можните напади и закани треба да се истражуваат, при што врз основа на добиените резултати од истражувањето ќе биде потребно да се креираат механизмите за заштита на информацискиот систем. Вообичаените закани во однос на сигурноста на информациските системи се однесуваат на пресретнување и измена на содржината на пораките, одбивање на услуга (*engl.* Denial of Service(DoS)), потоа одбивање на пристапот за користење на системот или некоја негова компонента итн.

Наведените пет постулати може да бидат употребени како основа за развој сервисно ориентиран информациски систем на највисокиот слој на соодветна „IT“ инфраструктура (види Слика 2). Со развој на информацискиот систем за разузнавање се постигнуваат минималните барања за дизајнирање на сервисите кои е потребно да бидат имплементирани во разузнавачкиот процес и неговите интерните функции, кои треба да бидат процесирани како надворешна точки на ИСР ([73]).

2.2 Пример за бизнис процес во сервисно ориентиран ИСР

На Слика 3 се претставени функциите на дистрибуираниот ИСР, кој треба да ги следи предложените постулати. Сликата претставува типичен пример за процес со внатрешните функции кои би требало да бидат воспоставени во разузнавачките сектори

или агенции. Процесот има три функции кои може да се процесираат од други надворешни ИСР точки во компјутерската мрежа ([73]).



Слика 3 Пример за бизнис процес во ИСР ([73])

Наведениот пример од Слика 3 претставува едноставен процес за кој би требало да се одвива во одреден сектор, институција поврзана со разузнавањето, каде се опишува процесот од праќање на барање за информација, па се до добивање на информацијата. Процесот содржи три функции кои би требало да се извршуваат од надворешни точки во „P2P“ мрежа.

Функција 1: Откако клиентот ќе побара информација, барањето треба да се прифати без разлика дали има доволно доволно податоци во системот за создавање на информацијата. Во случај кога нема доволно информации, барањето од клиентот треба да се третира како барање за креирање на информацијата од одредена агенција која ќе биде одредена за провајдер на информацијата. Неопходните влезни податоци кои треба да бидат пратени до надворешните точки ги вклучуваат сите податоци од барањето за информации. Врз основа на наведеното, функцијата прави пресметки со цел да се провери дали информацијата може да се прати директно до клиентот или се потребни дополнителни податоци за креирање на информацијата врз основа на барањето од клиентот. На крај надворешните функции враќаат информациска порака за локалниот процес.

Функција 2: Доколку не постојат доволно податоци во друг сектор, оддел, институција поврзана со разузнавањето од ИСР, оваа функција одредува кои се критичните побарување за да се создаде информацијата. Влезни вредности се: барањето за

инфомацијата, која разузнавачка дисциплина ќе употребува и кој ќе биде извршител. Откако влезните параметри се креирани, барањето за инфомации се проследува до одговорните агенции за разузнавање, при што започнува планирањето, собирањето и анализата на податоците за информацијата. Со цел да се поедностави процесот, ние претпоставуваме дека агенцијата која е носител на активноста ќе ја достави информацијата на време без можни проблеми. Вредноста која треба да се врати од надворешната функција е комплексен објект кој ги содржи сите податоци поврзани со разузнавачката информација и времето за нивно користење.

Функција 3: Кога има доволно податоци во секторот, креирањето на информацијата може да започне. Понатаму третата функција ги креира сите забелешки (*engl.* Data records), на пример, до кого е испратена информацијата, колку време може да се користи и ги обвиткува како комплексни објекти кои ќе бидат вратени назад до точката од ИСР која е барател на информацијата.

Локалната точка (*engl.* External peer) во примерот ги обвиткува бараните податоци како бизнис објекти кои се вклучени во далечинскиот повик на функцијата. Вратените комплексни објекти содржат дополнителни податоци кои се снимени во локалната база на секторот.

Примерот покажува како единечни функции на процеси се извршуваат на надворешен ИСР точки и како локалните точки и како локалниот ИСР систем ќе има корист од употребата на надворешната бизнис логика, на пример употреба на функцијата за оптимизација.

2.3 Цели на концептот

Цели кои се однесуваат на СОА концептот за развој на информациски систем за разузнавање се следните:

1. Предложениот модел на информациски систем за разузнавање овозможува задоволување на дисциплините, како и разузнавачкиот циклус на кои се базира разузнавањето во Р. Македонија.
2. Развој на модел, начин и метод за интеграција на апликациите на селектираните информациски системи со ИСР за потребите на разузнавањето во Р. Македонија
3. Истражување на можностите за искористување на соодветни стандарди со цел надминување на предизвиците од зависноста на информациските системи од еднообразната технологијата и воспоставување на информациски систем базиран сервисно ориентираната архитектура во целост
4. Предлог решение за имплементирање на СОА сигурносните стандарди ([72]), со цел да се постигне соодветно ниво на контрола на пристап и евиденција на корисниците.
5. Модел на ИСР кој содржи протокол дистрибуирано пребарување на информациите (online or near-line) во зависност од важноста на ситуацијата со цел да се донесе соодветна одлука од авторитетите.

ГЛАВА 3

ИМПЛЕМЕНТАЦИЈА НА СЕРВИСНО ОРИЕНТИРАНА АРХИТЕКТУРА ВО ПРОТОТИП НА ИНФОРМАЦИСКИ СИСТЕМ ЗА РАЗУЗНАВАЊЕ

Заради одржување на чекорот со современите развојни трендови, потребно е краткорочно, среднорочно и долгорочно планирање на финасиски средства за развој на информациските системи за поддршка на разузнавањето, во однос на развојот на информацискатa технологија.

Во ова поглавје е презентирана идеја за имплементација на СОА во прототип на информациски систем за разузнавање. Прототипот на информациски систем за разузнавање претставува идејно решение, кое треба да овозможи зголемена координација и ефикасност во разузнавањето, а воедно претставува основа за создавање на систем за ефективно интегрирано разузнавање.

3.1 Користење на сервисно ориентирана архитектура во информациски системи

СОА е технолошки пристап кон дизајнирање на информациските системи, каде што примарна цел е да се искористи развојот и достигнувањето на „IT“ во бизнис процесите, на начин на кој ќе се оствари поголема ефикасност, за да се создадат симбиотички и синергетски релации ([28], [29]). Но, исто така постојат голем број несогласувања дека со СОА ќе се решат голем број на технички проблеми и ќе се искористат придобивките од „NEC“ (Network Enabled Capability). Тоа е само делумно точно, бидејќи СОА решенијата сами по себе се производ на „IT“ и зависат од многу други фактори кои се дел од оперативниот процес, како на пример човечки или организациски фактор, како составни компоненти на одбранбениот систем на една држава. СОА претставува апстрактен концепт “service”, каде сервисот е технологија - независна структура која го поедноставува процесот преку „loose coupling“ и обезбедува основа за создавање компонентни (модуларни, отворени) архитектури.

На бизнис ниво, бизнис компонентите разменуваат „large-grained“ бизнис сервиси (т.е. приказ на целиот оперативен процес (*engl.* Common Operating Picture (COP)) ([22], [24]). На технолошко ниво, „fine-grained“ технолошките сервиси се разменуваат (т.е. зачувување на податоци). СОА претставува мост, преку кој се извршува мапирање на „large-grained“ бизнис сервисите во „fine-grained“ технички сервиси.

Моменталната ситуација укажува дека, министерствата за одбрана ([24]) не се во можност да постигнат флексибилност за комбинирање, распоредување и конфигурирање на софтверски компоненти на соодветен начин или пак да создадат одредени нови компоненти. СОА понудува архитектонска структура која обезбедува ниво на интеграција на сервисите, како сигурен патоказ за задоволување на софтверски и бизнис барањата, со цел за добивање на поквалитени продукти во работењето. Претходно наведеното го

оправдува инвестирањето во употребата на СОА, но вистинската оправданост е во подобрување на начинот на работа, синергетски промени и експлоатацијата на информациите ([25]).

Во првите фази на имплементирање на СОА, често е многу тешко да се одредат карактеристиките при развојот на интегрирани системи кои треба да се користат во воени цели ([13], [14]). Може да се заклучи дека сепак се доаѓа до одредена точка, каде што понатамошната интеграција и интероперативноста со користење на веќе постоечките системи претставува дополнителна предност. Во релативно напредни воени сервиси, имплементацијата на СОА или „Federated Enterprise Service Bus“ (ESB) е голема, при што групираните апликациите се претставени како множества на добро дефинирани сервиси (бизнис компоненти), така што постигнато соодветно ниво на оптимизација. Додека ова е јасно посакувано и генерално корисно достигнување, вистинскиот предизвик или можност за минстерствата за одбрана сега е концентрацијата во зголемувањето на употребата на корисни информации, заедно со флексибилноста и степенот на брзиот „re-engineering“ или создавање на компонети за повторна употреба кои поседуваат карактеристики за работа во сервисно-базирани околини.

3.2 Примена на „NEC“ во сервисно ориентиран информациски систем за разузнавање

Целта на „NEC“ (Networked Enabled Capability) е да поддржи донесување на одлуки преку „навремено обезбедување и користење на информации од разузнавањето“([20]). Имплементацијата на „NEC“ во доменот на безбедноста и одбраната е со цел зголемување на воената ефикасност.

Концептот за мрежата „NEC“ во поддршката на размена на информации е поинаков за разлика од решението на „Network - Centric environment“, каде што мрежата е јадрото на кој е изградена воената ефикасност. Користењето на концептот за „NEC“ ја нагласува важноста во донесувањето на одлуки од авторитетите во воениот домен, со информации кои се потребни за правилно донесување на одлука.

Од аспект на „IT“, имплементација на „NEC environment“ е предизвик. Како пример може да се наведе сценарио, каде постои потреба од дистрибуирање на податоци добиени од поголем број на сензори (беспилотни летала, борбени возухоплови и др. елементи од борбениот распоред) и истите е потребно да се разменуваат помеѓу различни штабови во заеднички операции.

Дополнување на предизвиците за дистрибуција на информациите преку „NEC“ е потребата за брз одговор на заканите. Врз основа на претходно наведеното може да се наведат следните шест карактеристики на „NEC“ ([21]):

1. Способноста за промена на работните процеси и способноста за организациска промена (*engl.* Adaptiveness);
2. Способност да се користат повеќе начини за беспрекорно функционирање (*engl.* Flexibility);
3. Способноста за правање на нови работи и старите работи во нови начини (*engl.* Innovation);
4. Способност за повторно правилно функционирање предизвикано од грешки (*engl.* Resilience);
5. Способноста за реакција на промените во околината на соодветен начин (*engl.* Responsivness);

6. Способноста за ефикасна работа (*engl.* Robustness).

Во услови на промена на заканите, ИСР мора да се адаптира, со цел рационално искористување на можностите што ги нуди „NEC“. Во информацискиот систем за разузнавање, се содржани извештаи, прегледи, проценки, анализи и други разузнавачки продукти во функција на процесот за донесување на одлука.

Тоа значи дека „NEC“ е значајно решение за ИСР, бидејќи овозможува поврзување на елементите на разузнањето кои остваруваат меѓусебна интеракција во оперативната средина ([23]). Потребите за пристап до информациите се следни:

- правовремена информација за поддршка на процесот за донесување одлука. (заради избегнување на преоптоварување со информации);
- пристап до информации во вистинско време во процесот за донесување одлука;
- висок квалитет (во однос на достигнување на безбедноста на информациите).

Од оперативен аспект, ефикасно искористување на информациите во поддршка на донесувањето на одлука во рамките на воената средина е клуч за воениот успех.

Како што воените закани се менуваат, а нови способности се развиваат (на пример, сензори и други средства) значи дека е потребна промена во праксата, од што произлегува дека ќе биде потребно ИСР да се развива на повисок стадиум со текот на времето.

Заради задоволување на новите оперативни барањата на клиентите, во овој труд е искористена е сервисно - ориентирана архитектура за креирање на ИСР.

СОА решението во ИСР треба да ги понуди следните можности:

- поврзување на бизнис процесите со технички сервиси за размена на информации;
- поддршка во флексибилни информациски механизми за размена;
- експлоатација на развојот на комерцијална технологија и отворените стандарди за да се овозможи хетероген систем;
- можност за зголемување на способноста преку системска интеграција и воведувањето на нови сервиси

Целта е да се овозможи пресретнување на клиентските барања и да се подобри воената ефикасност.

3.3 Прототип на информациски систем за разузнавање

Во прототипот на ИСР потребно е да обезбедат соодветни алатки за поддршка на процесот на донесување на одлуката со цел да се подобри оперативната ефикасност според следното:

- користење на соодветен пакет алатки за дигитални поддршка при одлучувањето;
- подобрено запознавање на персоналот со елементите на борбениот распоред на заканата;
- способност за комбинирано и заедничко дигитално планирање;
- можност за флексибилен, интегриран и брз начин на проток на информации;
- можност за координација, синхронизација и извршување низ цел спектар на активности за поддршка на мисија;

- можност за подобрено менаџирање со информациите со користење на „NEC“.

3.3.1 Типови корисници

Типовите корисници што постојат во ИСР може да се разгледуваат од два аспекта, и тоа:

- аспект на ИСР системски функционалности;
- аспект на ИСР кориснички функционалности.

Аспектот на ИСР системски функционалности дефинира стандардни корисници од системски аспект. Тоа се следните типови на корисници:

- Администратор на комуникациска инфраструктура;
- Администратор на апликациско решение (дефиниција на веб сервиси, интеграција во информациските системи на институциите);
- Сигурносен администратор (дефинирање на полиси).

Овие типови корисници се стандардни типови на корисници кои постојат во било кој покомплексен информационен систем. Од функционален аспект ИСР има дополнителни четири типови корисници (види Слика 4):

- Корисник на услуги
- Сервис провајдер
- Компании
- Разузнавање (IMINT, SIGINT, OSINT, MASINT)

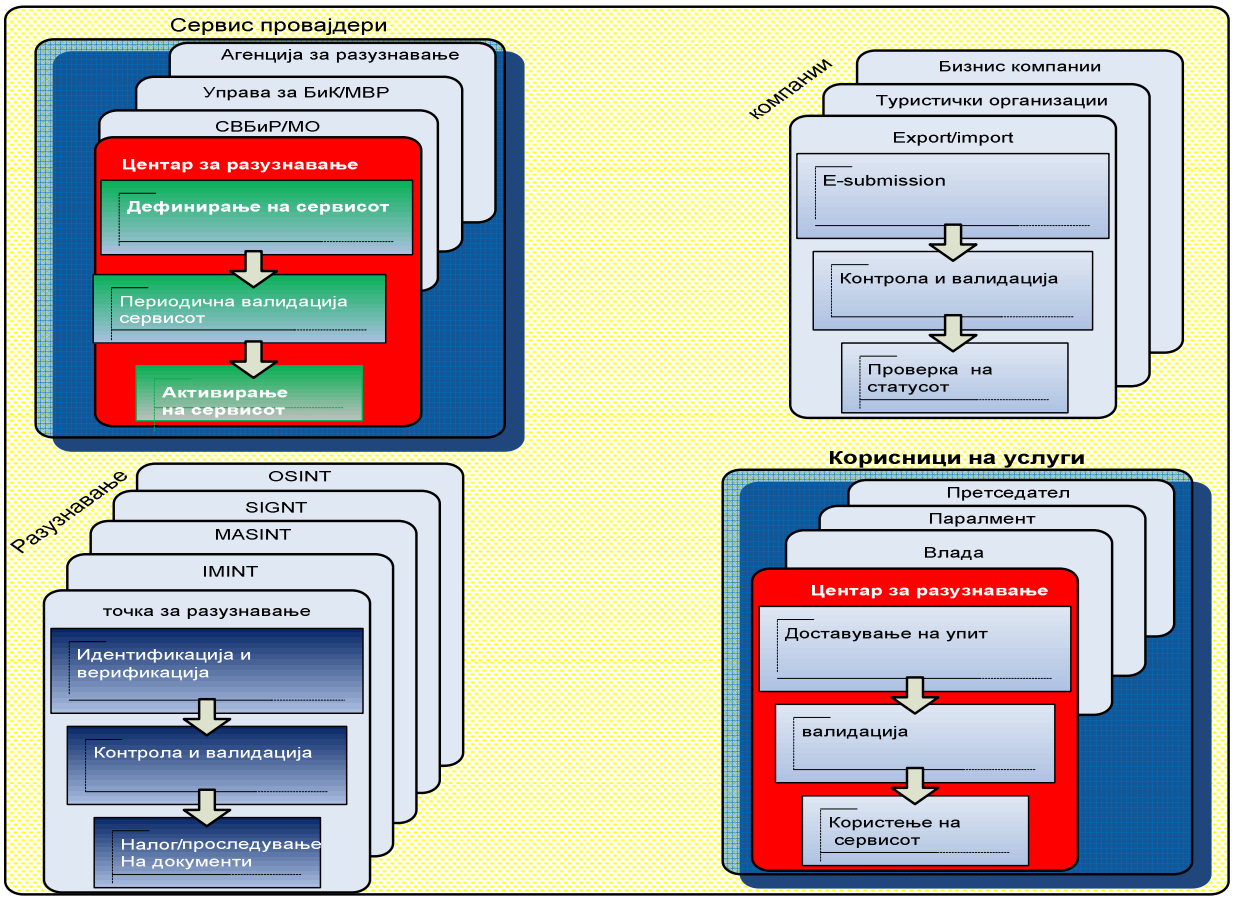
Корисник на услуги се однесува на било која институција (Центар за Управување со кризи, МВР, Агенција за Разузнавање и други институции) кој за потребите на својата работа има потреба да добие информација, или да достави информација (како налог или нотификација).

Сервис провајдер е корисник кој треба да обезбеди информација (при што може да побара соодветно овластување во согласност со сопствените сигурносни процедури или пак во согласност со некои надворешни нормативи (при што тоа треба да го оствари како побарување на услуга од ИСР)).

Компании се надворешни корисници кои можат да бидат проследени директно до некоја институција која го реализира нивното побарувања (пример Управа,Сектор или Одделение на Влада), но може да побараат и некои јавно достапни информации кои треба да бидат одобрени и обезбедени од ИСР.

Разузнавањето се базира на четирите разузнавачки дисциплини: „IMINT“, „SIGINT“, „MASINT“ и „OSINT“. Исто така дисциплините се разделуваат на поддисциплини со различни специфичности во делокругот на работата и може организационо да припаѓаат на повеќе институции или единици во состав на Одбранбените сили на државата (Агенција за разузнавање (АР), МВР, МО, Министерство за Здравство, МНР и други субјекти), но нивната улога и задача е да внесуваат податоци (информации, проценки, анализи, извештаи и др.), прават нивна верификација (што може да биде предмет на поддршка на ИСР) и добиваат нотификации или налози (на пример за политичко-безбедносната состојба во одредена држава во однос на сигурноста на инвестицијата).

На Слика 4 е даден приказ на овие кориснички типови како и поделбата по фази на нивните генерални кориснички функции.



Слика 4. Корисници на системот за поддршка на разузнавањето

3.3.2 Сервисно ориентирана архитектура на ИСР

Сервисно ориентираната архитектура на ИСР треба да обезбеди централен систем за поддршка на разузнавањето од логички аспект, додека неговата физичка поставеност да е дистрибуирана.

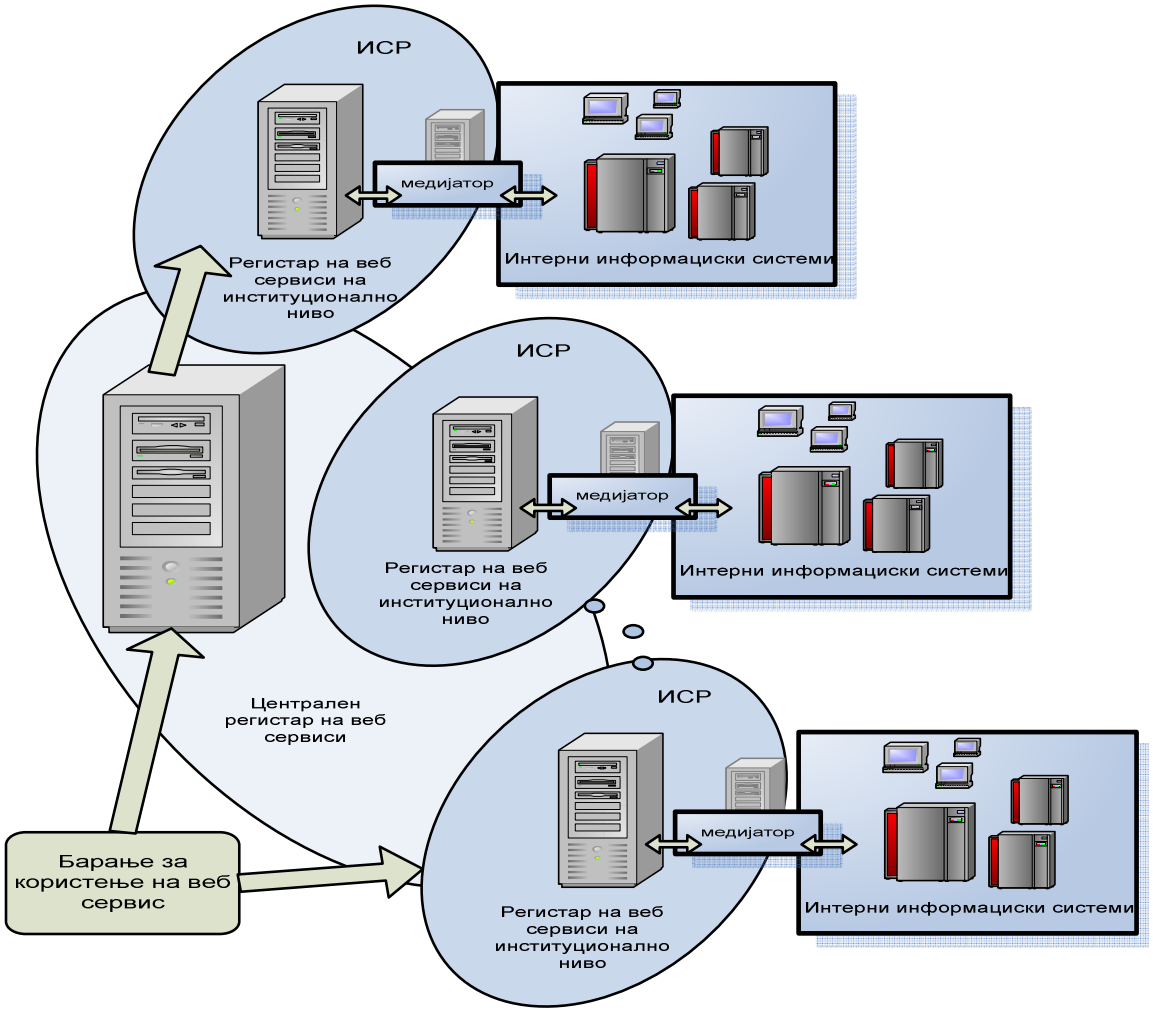
Сервисно ориентираната архитектура на ИСР ќе биде опишана преку елаборирање на логичката архитектура на ИСР и слоевитата архитектура на ИСР.

3.3.2.1 Архитектура на сервисни регистри

Веб сервисите се самоопишувачки компоненти кои се овозможени нивните сервиси преку Интернет протоколи. Комуникацијата преку интернет значи отвореност на тие сервиси. Секој корисник може да пристапи кон регистрирани веб сервиси од било кој компјутер поврзан на интернет. Единствено што треба да знае е како да го најде сервисот што го бара, т.е. треба да знае како да го открие. Вакво откривање може да се изврши со помош на „UDDI“ регистри ([12]), како што е прикажано на Слика 5.

Откривањето на веб сервиси е процес на наоѓање на адекватен веб сервис за дадена активност. Публикување на веб сервис вклучува во најмала рака креирање на софтверски артефакт и негово ставање на располагање на потенцијалните клиенти. За софтверот да може да го користи сервисот, провајдерите вообичаено ја надополнуваат страната кај веб

сервисот со опис на интерфејсот користејќи го „Web Services Description Language (WSDL)“.



Слика 5. Архитектура на сервисни регистри на ИСР

Опционално, провајдерот може експлицитно да регистрира сервис на регистер на веб сервиси како на пример „UDDI“ или да публикува дополнителни документи наменети во функција на откривање, како на пример „Web Services Inspection Language (WSIL)“ документи. Корисниците на сервисот или клиенти треба да го пребаруваат сервисот рачно или автоматизирано. Имплементацијата на „UDDI“ сервисите и „WSIL“ алатките треба да овозможат едноставни програмски алатки или веб базирани кориснички интерфејси (GUI) да помогнат во наоѓање на веб сервиси ([76]).

„UDDI“ регистерот прифаќа информации кои го опишуваат процесот од интерес, вклучително и веб сервисите кои ги нуди, но исто така овозможува заинтересираните страни да направат пребарувања и превземања на информацијата.

На Слика 5 е прикажано јавен „UDDI“ сервис кој е хостиран од повеќе институции вклучени во процесот на разузнавање. Секоја институција овозможува јавно достапна база која содржи регистарски податоци за бизниси кои се овозможени преку „SOAP“ барања до

податочните центри на институциите. „UDDI“ регистрите можат да бидат реплицрани и кај секоја од институциите.

„UDDI“ дефинира множество на стандардни интерфејси за пристап до база од веб сервиси. Базата содржи записи за веб сервисите, како и за други „UDDI“ елементи. „UDDI“ елементите, се информациски структури кои се зачувани во „UDDI“ регистер и вклучуваат специфични технички информации. Тоа може да се типови на веб сервиси, нивните категории за пребарување, бизнис ентитети на кои им припаѓаат сервисите, итн.

„UDDI“ овозможува два типа на програмерски интерфејси (API) за пристап до „UDDI“ регистер. Упитни интерфејси се користат за пребарување на општите „UDDI“ елементи како на пример процеси, сервиси, сервисни типови и спојни темплејти кои овозможуваат и ги нудат пристапните информации за сервисите. Публикувачки интерфејси овозможуваат методи за публикување (регистрација) на „UDDI“ елементи и веб сервиси.

Треба да се забележи дека „UDDI“ регистерот не чува компоненти од веб сервиси, ниту како код ниту како модули. Кога се зборува за публикување на веб сервиси во регистер, се мисли дека „UDDI“ регистер креира само запис за веб сервисот, негова пристапна точка и линк до „WSDL“ документи ([55], [56], [57]).

Откако веб сервисот е изграден и имплементиран, следниот чекор е објавување на овој сервис со цел другите корисници да можат да го откријат и да работат со него. Јавните „UDDI“ регистри го нудат ова.

Функционалната цел на „UDDI“ регистер е репрезентација на податоци и метаподатоци за веб сервиси. Тој претставува регистер наменет за користење во рамките на јавна мрежа или во рамките на интерна мрежа на организација, и нуди стандардизиран механизам за класифицирање, категоризирање и менаџирање на веб сервиси за тие, да можат да бидат откриени и искористени од друга апликација.

Согласно на тоа, стандардот специфицира протоколи за пристап до регистерот за веб сервисите, методи за контрола на пристап до регистрите и механизам за дистрибуирање или делегирање на записи до други регистри. Со други зборови, стандардот овозможува начини за лоцирање на веб сервис, негово повикување, и менаџирање на мета податоците за тој сервис.

Клучни функционални концепти за работа со „UDDI“ вклучуваат:

- „UDDI“ податочен модел. „UDDI“ спецификација дефинира основни податочни типови кои вклучуваат опис на бизнис функционалноста на сервисот, информација за тоа кој ја објавил услугата, технички детали за сервисот и програмерски интерфејси (API). Овие податочни типови се дефинирани во неколку „XML“ шеми, кои заедно оформуваат основен информационен модел и рамка за интеракција помеѓу „UDDI“ регистри. Во продолжение овие типови се излистани;
- Опис на бизнис функционалности на сервисот за сервисите со кои ќе се тестира функционалноста на ИСР;
- Информација за организацијата која го публикувала сервисот;
- Техничките детали за сервисот, вклучувајќи и референци до програмерските интерфејси на сервисите (API);
- Разни други атрибути или метаподатоци како на пример таксономија, транспорти, дигитални потписи;
- Релации помеѓу ентитети и нивни регистри;

- Стандардни барања за следење на промена во листа на ентитети;
- Дефинирање на „UDDI“ јазли и регистри. „UDDI“ вклучува и специфична дефиниција за хиерархиски однос помеѓу една инстанца од „UDDI“ имплементација и другите со кои е поврзан. Технички, постојат три главни класификации на „UDDI“ сервери:
  - ❖ Јазел е „UDDI“ сервер кој подржува барем минимален сет на функционалности дефинирани во спецификацијата. Тој може да извршува една или повеќе функции на „UDDI“ податоци до кои има пристап. Тој е член на точно еден „UDDI“ регистер;
  - ❖ Регистер е содржан од еден или повеќе јазли. Регистер изработува комплетен сет на функционалности дефинирани во спецификацијата;
  - ❖ Придружни регистри се индивидуални „UDDI“ регистри кои имплементираат меѓусебно делење на податоци според полиси. Придружни регистри делат сроден именски простор (namespace) за „UDDI“ клучеви кои уникатно ги идентификуваат податочните записи.
- Есенцијални програмски интерфејси. „UDDI“ регистер овозможува неколку клучни функции кои вклучуваат:
  - ❖ Публикување на податоци за сервис во регистер;
  - ❖ Пребарување на „UDDI“ регистер за информации за сервис.
- Како повеќекратни регистри може да формираат група позната како афилијација, да дозволи полисно базирано меѓусебно копирање на основни податочни структури. Некој од најважните концепти кои подржуваат интеракција помеѓу регистри вклучуваат:
  - ❖ Репликација и пренос на сопственост на податоци за сервис;
  - ❖ Менаџирање и генерирање на регистрациски клучеви;
  - ❖ Сет на регистрациски програмерски интерфејси;
  - ❖ Безбедност и авторизација.

3.3.2.2 Логичка архитектура на ИСР

На Слика 6 е претставена предложената логичка архитектура на системот за подршка на ИСР. Таа го користи слоевитиот модел и се состои од следните слоеви (нивоа):

- Ниво за корисници
- Ниво за пристап
- Ниво за процеси
- Ниво за услуги (сервиси)
- Ниво за обезбедувачи на услуги (сервиси)

Нивото на корисници обезбедува пристап преку користење на соодветна презентациска логика до ИСР за сите типови на функционални и системски корисници елаборирани во секцијата (3.1 Типови на корисници). Од организационен аспект тие типови корисници припаѓаат на: центарот за разузнавање, ЦУК, амбасади на МНР, и други владини институции и агенции, но може да бидат и надворешни корисници претставени преку компании.

Овие корисници согласно сигурносните полиси имаат различен начин на пристап до ИСР. Начинот на пристап се дефинира во нивото на начин на пристап. Тој може да

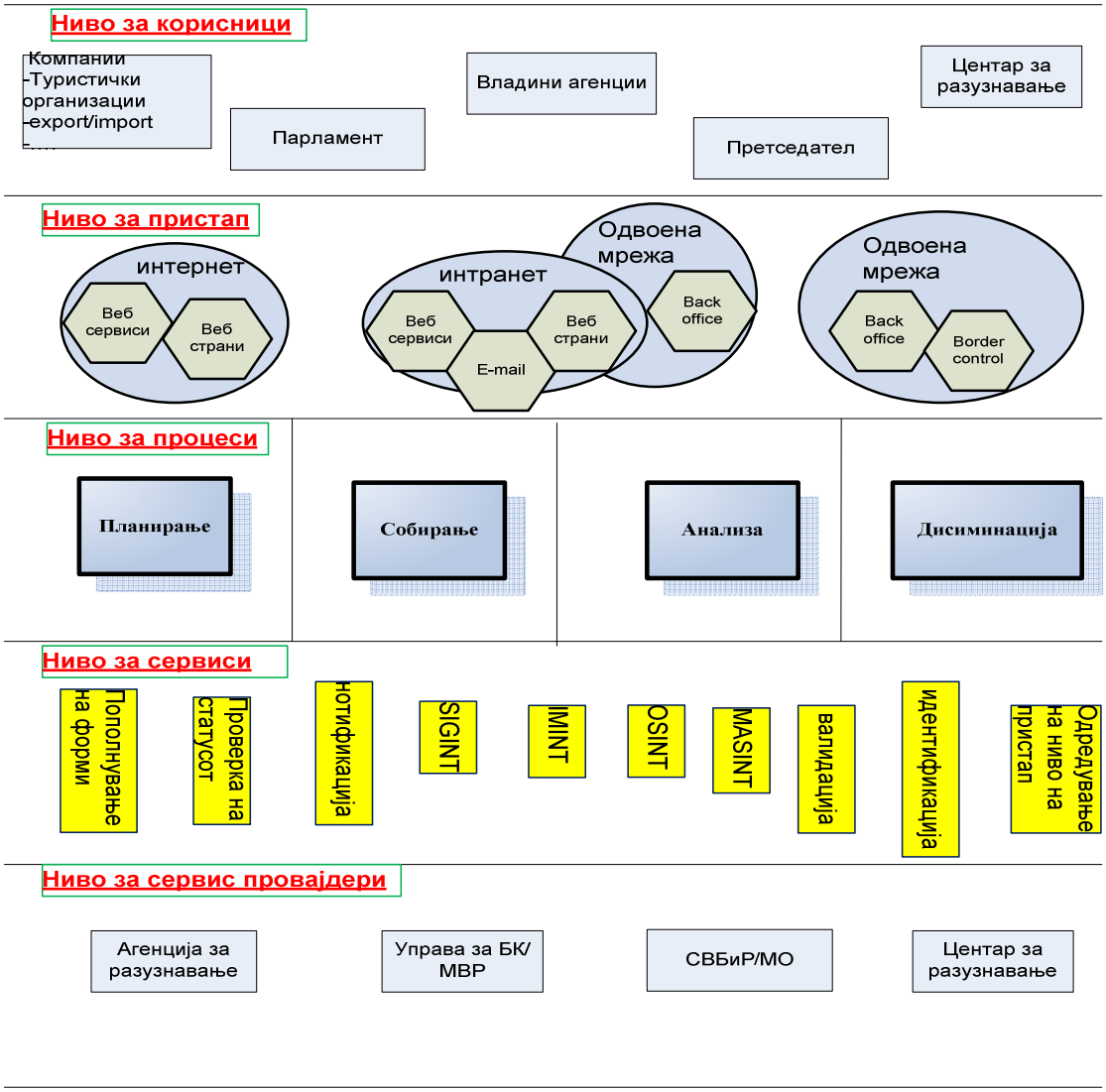
биде преку јавната интернет мрежа (електронска пошта, пристап до веб порталот на ИСР), приватна интранет мрежа (преку веб страници, електронска пошта, но и интеграција со информациските системи што постојат во институциите), или пак одделена приватна мрежа (преку проширување на системот на МО, МВР и другите учесници со можност за користење на услугите на ИСР, и интеграција во делови на информациските системи кои имаат посебна важност за работата на институциите). Нивото на пристап, во согласност со дефинираните полиси на типовите на корисници го одредува начинот на пристап на секој корисник.

Од начинот на пристап зависи множеството на расположиви процеси од доменот на разузнавање до кој корисникот ќе има пристап. Можни процеси се: планирање, собирање, анализа и десиминација. Овие процеси во себе обединуваат цела хиерархија на можни сценарија на користење кои зависат од законските и интерните регулативи на институциите вклучени во процесот на разузнавање ([74],[75]).

Сервисите кои се користат се дефинирани во нивото на услуги (сервиси). Тие се достапни за интеграција во процесите што се користат од корисници, а кои во согласност со сигурносните полиси и пристапни точки имаат право да ги користат. Такви сервиси можат да бидат: сервиси на проверка (дали компанија или документ постои како ставка во некоја база на податоци), сервиси за собирање податоци (IMINT, SIGNT, OSINT и MASINT), одредување (и промена) на право на пристап согласно некоја регулатива (што подразбира автоматизиран или мануелен процес на одобрување), идентификација (дали дадено лице или документ соодветствува со тоа што се претставува врз основа на правило (споредба на податоци, статистичка анализа)), пратење (на добра со помош на „GPS“ уред), нотификација (за учество во заедничка контрола, за статистичка евиденција, за ажурирање на географски информационен систем врз основа на сигнал од „GPS“ уредот), пополнување на формулари (за добивање на информации, проценки, извештаи и слично), проверка на статус на одредени барања (дали барањето е евидентирано, се разгледува или е одобрено).

Сите сервиси произлегуваат од соодветни обезбедувачи на услуги претставени преку информациските системи на министерствата, институциите и агенциите вклучени во процесот на разузнавање. Дозволено е обезбедувачи на услуги да бидат и други системи за поддршка на меѓуиституционално управување. Обезбедувачите на услуги преку системот за поддршка на „workflow“ процеси дефинираат нови веб сервиси кои ги стават на располагање на сите корисници со обезбедено право на пристап до соодветните регистри на сервиси ([30],[31]).

На тој начин се обезбедува флексибилна архитектура која обезбедува постојано проширување и ажурирање на множеството на сервиси кои се на располагање на корисниците на ИСР. При тоа се води сметка за сигурносните полиси, но најважно од сè, се постигнува пристап до информации на униформен начин преку множество на пристапни точки што претставува својство на централизиран систем. Поради тоа предложената архитектура на ИСР е централизирана од логички аспект.



Слика 6. Нивовска логичка архитектура на системот за поддршка на ИСР

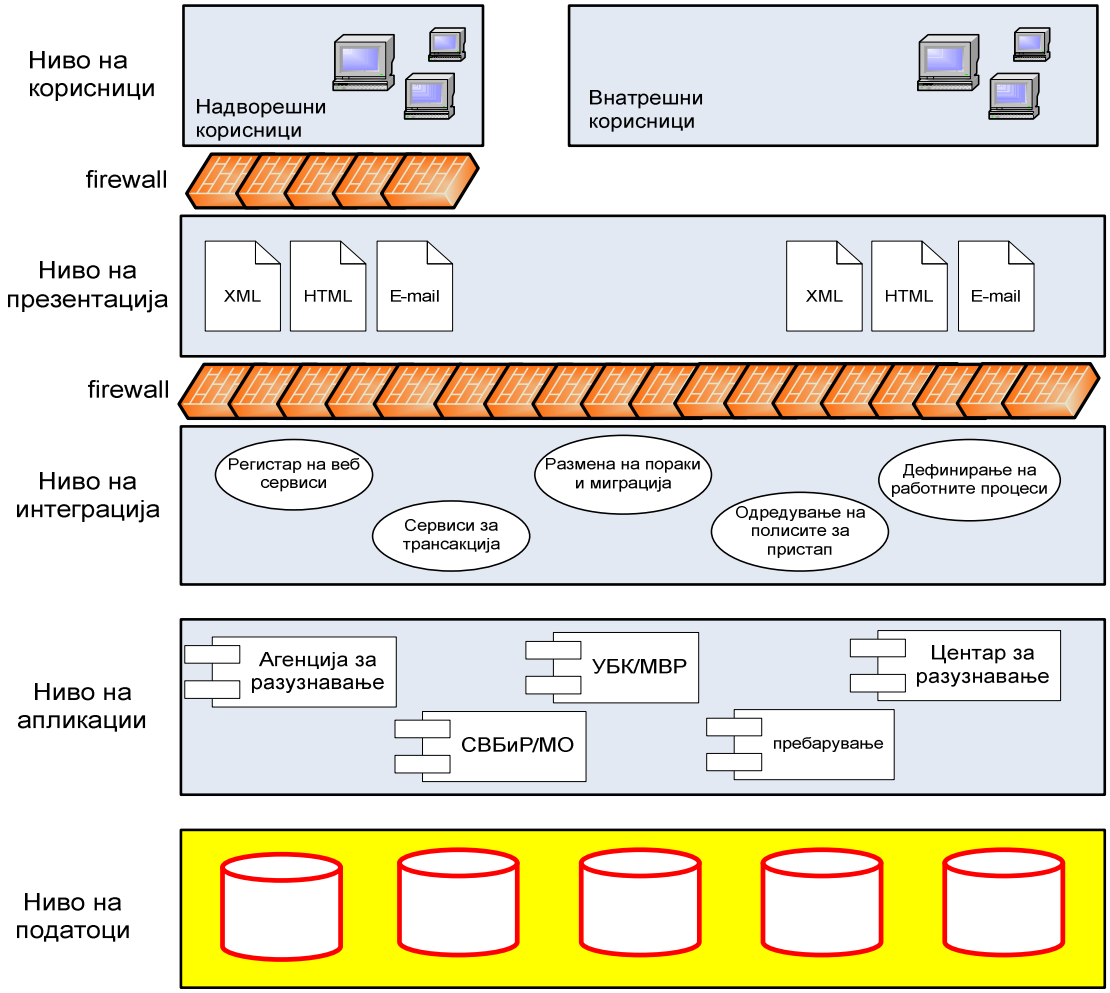
3.3.2.3 Архитектура на ИСР

Генералната архитектура на прототипот ИСР е дадена на Слика 7. Поради комплексноста на системот таа е реализирана како слоевит модел на архитектура на информациски систем.

На најниско ниво постои дистрибуиран систем од хетерогени бази на податоци кои немаат заеднички систем за управување со бази на податоци, па како такви тие не се од директен интерес на системот на ИСР. Отстапка од оваа констатација е базата на податоци која ќе го евидентира користењето на сервисите обезбедени од ИСР, а ќе биде под надлежност на центарот за координација на ИСР.

Пристап до одделните бази на податоци во принцип се прави со апликацискатa логика на модулите кои припаѓаат на интерните информациски системи на институциите вклучени во ИСР. Тие апликации треба да обезбедат интерфејси до нивото на интеграциска логика.

Нивото на интеграциска логика е клучно за реализација на ИСР. Тоа ниво треба да обезбеди креирање на сервиси преку медијаторски алатки за пратење на процеси (*engl.* workflow) кои ќе бидат поврзани со постоечките модули на интерните информациски системи и нивна трансформација во веб сервиси. Интеграциското ниво треба така добиените веб сервиси да ги публикува во соодветни регистри на веб сервиси во зависност од привилегиите за пристап. Ова ниво управува и со привилегиите за пристап, како и за размена и прилагодување на пораки од различни извори, во случај на потреба од нивно донесување во компарабилен формат. Конечно, ова ниво се грижи за управување на услугите понудени од ИСР во вид на трансакции доколку е тоа потребно. Со една реченица, ова ниво ја обезбедува функционалноста на сервисите во ИСР.



Слика 7. Архитектура на прототип систем за поддршка на ИСР

Тие сервиси треба да бидат достапни до различни категории на корисници. За потребите на заштита на ИСР, позади ова ниво треба да е инсталиран заштитен ѕид (*engl.* firewall) после кој следи нивото на презентациска логика. Ова ниво може да биде реализирано во форма на портал кој нуди: листа на веб сервиси преку пристап до сервисни регистри, интеграција на веб сервисите со електронска пошта или директно како оддалечен процедурален повик на апликациите (*engl.*Remote Procedure Call (RPC)) во

стандардизиран формат „XML“, но и како обичен „HTML“ текст за одредено множество на сервиси односно корисници.

Надворешните корисници на системот се одделени со уште еден дополнителен заштитен ѕид (*engl.* firewall), со што се постигнува максимална заштита од несакани продирања во системот.

ГЛАВА 4

МОДЕЛ НА РЕШЕНИЕ ЗА ИНТЕГРАЦИЈА НА ИСР СО СОА БАЗИРАНИ ИНФОРМАЦИСКИ СИСТЕМИ

Информацискиот систем за разузнавање е креиран со цел да ги задоволи поединечните разузнавачки функции. Корисниците на системот се дел од одреден оддел, секција, сервис или агенција со различни специфичности во работата во функција на задоволување на процесите во разузнавачкиот циклус.

Размената на информации и нивната употреба од различни корисници, во зависност од сигурносните полиси кои ги имаат за пристап во информацискиот систем, овозможува подобрување во процесот на донесување на одлуки од страна на авторитетите. Исто така им овозможува полесно да ги планираат идните чекори. Со цел да се постигне што подобра размена на информации и нивна достапност до корисниците, потребно е да се развие модел за интеграција на информациските системи, кој ќе овозможи интеграција на информациски системи базирани на различни технологии и различни интеграциони платформи ([3]).

Во ова поглавјето се разработени намената и функциите на информациските системи за кои се проценува дека се потребни за интеграција со ИСР, потоа даден е преглед на модели за интеграција на апликациите и на крај е презентиран модел на соодветно решение за интеграција со различните информациски системи кои се користат во институциите.

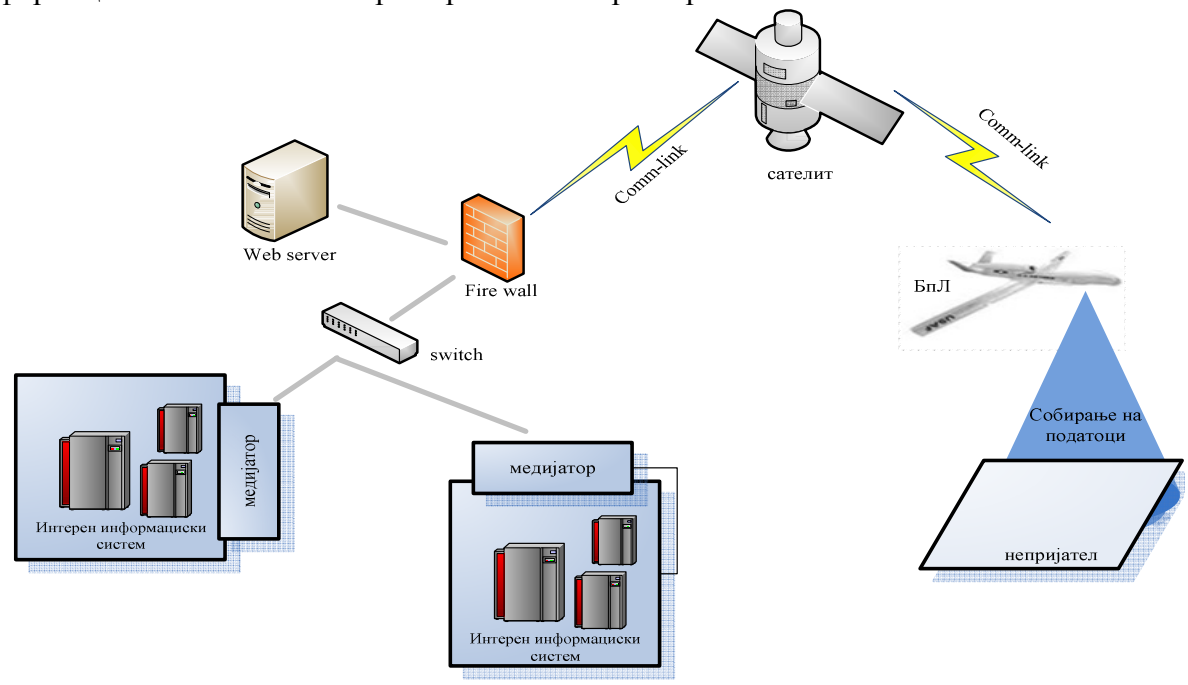
4.1 Потреба од интеграција на ИСР

Заради извршување на основната функцијата за која се креира, потребата од интеграција со различните информациски системи неминовно се наметнува. Интегрирањето со други информациски системи ќе овозможи подршка во процесот на разузнавањето ([27]), бидејќи планирањето, собирањето, анализата и десиминацијата на податоци како есенцијални процеси во разузнавачкиот циклус во потполност ќе се задоволат.

Информациските системи со кои ИСР се интегрира, ќе се појават и како провајдери на сервиси и како корисници на сервисите од ИСР ([44]). Односно, доколку е потребна одредена разузнавачка проценка за авторитети кои се корисници на одреден информационен систем, тогаш сервисите од ИСР, во согласност со тековните сигурносни полиси, треба да бидат достапни. Во наведениот пример, ИСР преставува провајдер на сервиси. Но, доколку е потребно, на пример проверка за одредено лице кое ја напуштило територијата на Р. Македонија, тогаш за ИСР ќе бидат користени одредени сервиси од друг информационен систем, во согласност со тековните сигурносни полиси, при што истиот ќе се појави како провајдер на информации.

Може да се набројат низа на примери кои укажуваат на оправданоста од интеграцијата на ИСР со други информациски системи.

Исто така, потребно е да се напомене потребата од интеграција (Слика 8) со високо технолошки средства (беспилотни летала, разни сензори, воздухоплови, сателити и друго) ([1]), во однос на интеграција во реално време и користење на сервиси заради добивање на информации кои се со лимитиран временски карактер.



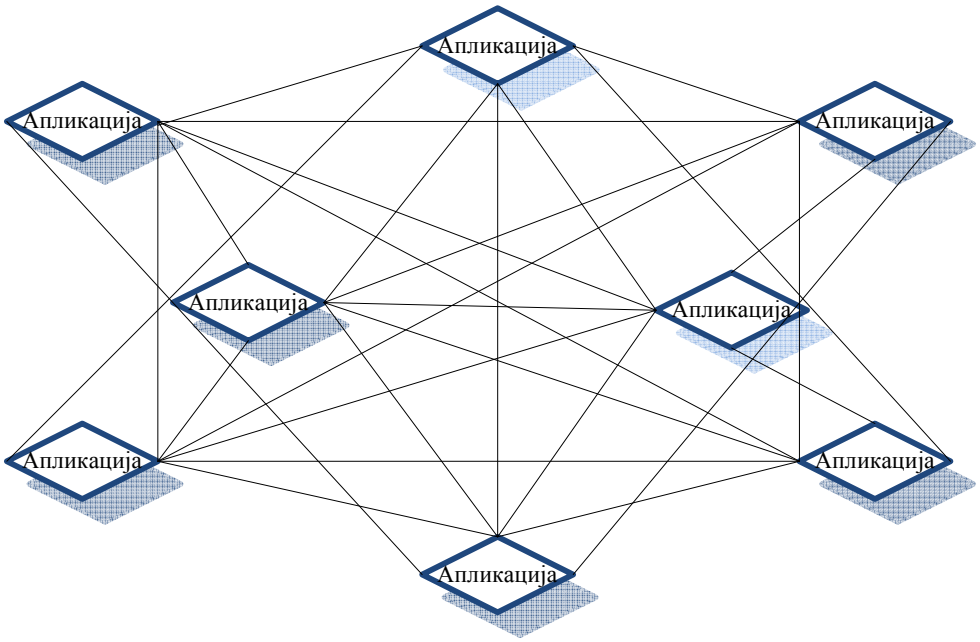
Слика 8. Интеграција на ИСР со високо технолошки средства

Интеграцијата е придобивка за „B2B“ процеси исто толку колку што е и за внатрешни бизнис процеси во самиот систем. Наведените примери, односно потребата за интеграција се фокусира на динамичните меѓубизнисни интеракции ([7], [9], [10]). Заради задоволување на потребите потребни се решенија за интеграција како “апликација-кон-апликација“.

4.2 Модели на интеграција на апликации

Интеграцијата на апликациите може да се реализира преку три концептуални модели, начелно по следното: поврзување точка – до – точка (*engl.* point-to-point), со примена на централен насочувач или посредник (*engl.* hub-and-spoke) и со примена на веб сервисни апликациски адаптери во COA ([77]).

Моделот на поврзување точка-до-точка претставува традиционален начин на интеграција на апликациите, каде што секоја апликација поединечно се поврзува со секоја апликација со која мора да разменува податоци. Концептуалниот модел на поврзување е преставен на Слика 9.



Слика 9. Интеграција на апликациите по моделот точка-до-точка ([18])

Ако $A_1, A_2,\ A_3 \cdots A_n$ се апликации во информациски систем, тогаш:

$$\mathrm{M} = \{A_1, A_2, A_3 \cdots A_n\} \tag{4.1}$$

е множество на тие апликации. Бројот на конекции помеѓу сите апликации во информацискиот систем е:

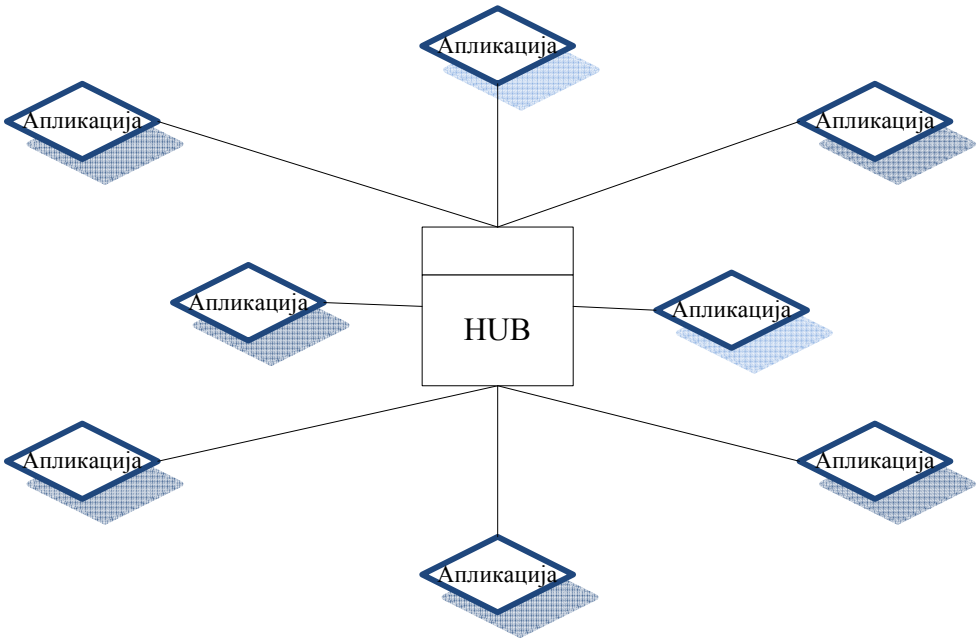
$$\mathrm{N} = n(n-1) \tag{4.2}$$

При тоа посебен проблем претставува различниот механизам на комуникација и форматот на податоци кој се користи од различните апликации.

Опишаниот начин на интеграција на апликациите бара долго време на интеграција, сложено одржување со многу големи финансиски трошоци. За да се поедностави комуникацијата помеѓу апликациите се развива модел во кој се применува централен насочувач или посредник (Слика 10). Во моделот со централен посредник се применува компонената која ги проследува пораките помеѓу апликациите. Централниот посредник ги прифаќа пораките од апликациите на испраќачите и ги проследува до апликациите на примателите.

Освен насочувањето на пораките централниот посредник ги извршува и потребните трансформации како во форматот така и во содржината на пораката.

Основниот недостаток при интеграција на апликациите по моделот со централен посредник е можноста посредникот да стане комуникациско тесно грло (*engl*. bottleneck), при што ќе се предизвика намалување на перформансите на информациско – комуникацискиот систем.



Слика 10. Интеграција на апликациите по модел на централен посредник ([18])

Заради надминување на воочените недостатоци на претходно наведените модели, моделот на интеграција на апликациите со веб сервис апликациски адаптери и употреба на концептот на СОА, преставува едно од решенијата кои во моментот дозволуваат комуникација помеѓу апликациите и најголемо искористување на перформансисте на информациските системи.

4.3 Веб сервис технологии

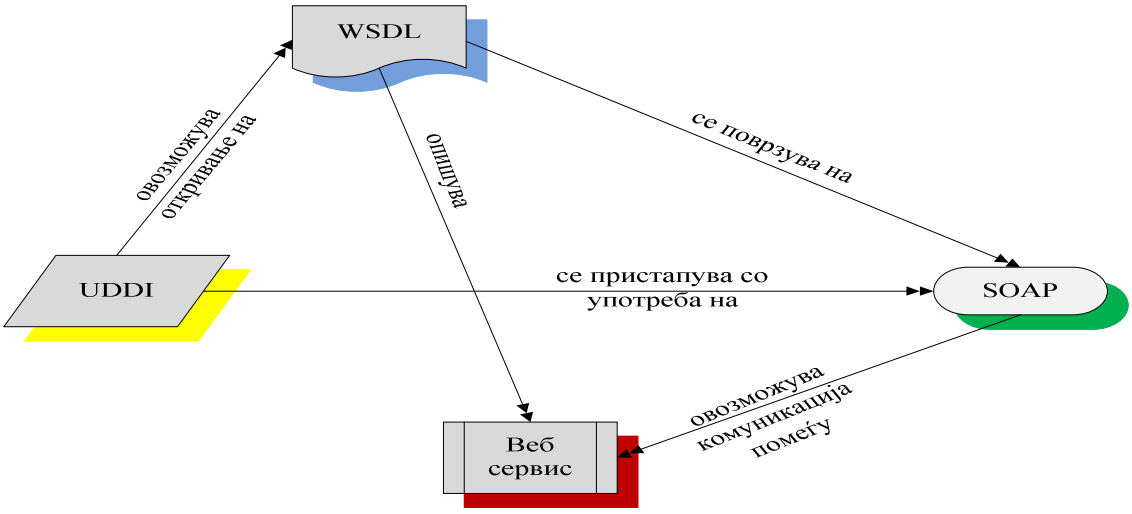
СОА е архитектура користена за подржување на „application-to-application“ интеграцијата, при што истата преставува основа за повеќето „RPC middleware“ системи, вклучувајќи ги „DCOM“, „CORBA“, „RPC“, „RMI“. За да се подржи наведеното решение и да се изврши интеграција со информациските системи, односно со софтверските компоненти, ќе биде потребно да се креираат веб сервис апликациски адаптери.

Веб сервис (чии составни делови се прикажани на Слика 11) е сервисно ориентирана апликација која комуницира преку веб користејќи „XML“ пораки. Веб сервисите ја претставуваат поврзаноста на трите основни технологии: „Web“, „XML“ и СОА. За да се обезбеди универзална поврзаност на субјектите, се користи „Web“ кој обезбедува основната инфраструктура која ги подржува веб сервисите. „XML“ е основата на „Web“-от. Било која апликација, напишана во било кој јазик, може да разбере „XML“, кој е флексибилен и адаптибилен јазик.

Специфицираниот механизам за опишување, рекламирање и истражување на сервисите и комуницирање со истите, може да се изведе со технологии користени за имплеметирање на овие функции во веб сервисите како „WSDL“, „UDDI“ и „SOAP“.

„WSDL“ е „XML“ јазик за опишување на веб сервисите. „WSDL“ документот опишува што прави сервисот, како комуницира и каде да се најде истиот. Може да се компајлира „WSDL“ документ и да се генерира „proxy“ на клиентот, кој го содржи целиот код кој е потребен за коминикација со сервисот.

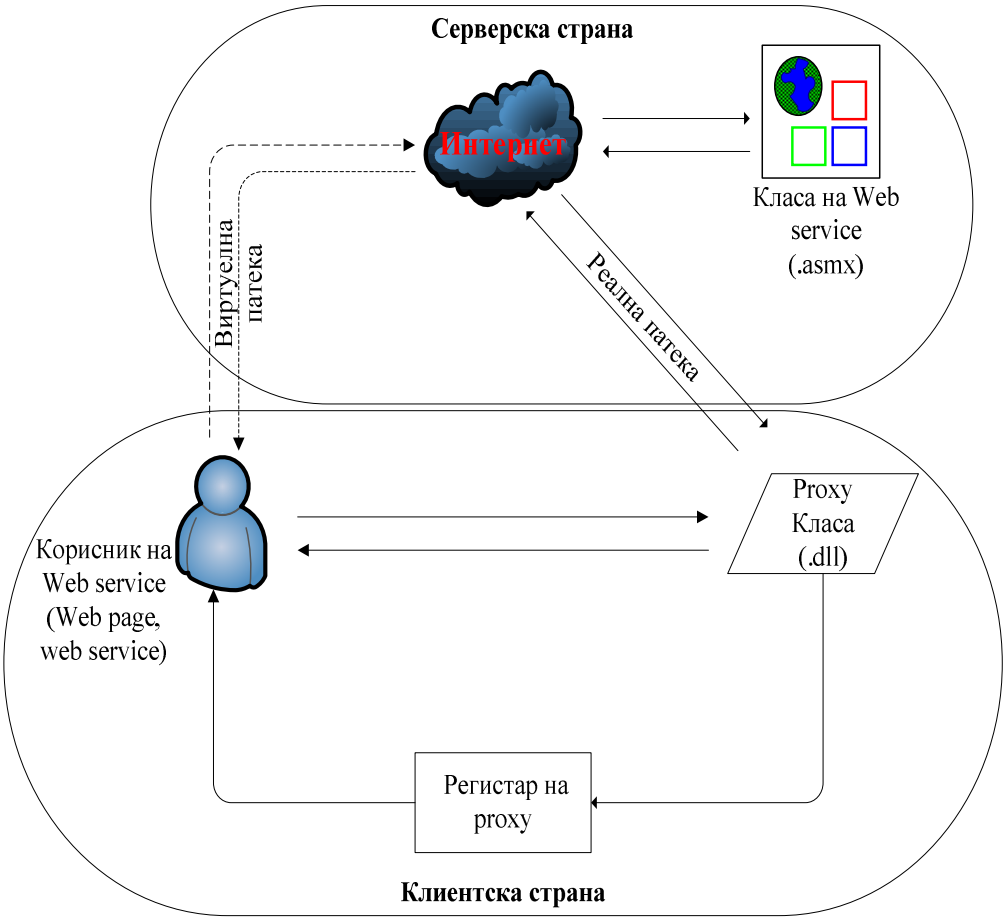
„SOAP“ е „XML“ протокол кој се користи за комуникација меѓу веб сервисите. „SOAP“ обезбедува едноставен, конзистентен и продолжен механизам кој овозможува една апликација да испрати „XML“ порака до друга аплиакција. „WSDL“ описот поврзан со веб сервисот ја дефинира структурата на „XML“ пораката.



Слика 11. Поврзување на технологиите за веб сервиси ([17])

Заедно, овие технологии имплементираат проширлива, лесна категорија на СОА инфраструктура. Веб сервисите ги земаат сите најдобри одлики на СОА и ги комбинираат со „Web“ и „XML“. Резултатот е архитектура која ги елиминира „Traditional Middleware Blues“ (не подржуваат хетерогеност, не работат со интернет, поврзани се со конекција „tightly coupled“). Веб сервисите подржуваат хетерогена и флексибилна интеграција.

Принципот на работа на веб сервисот (Слика 12), се состои во праќање на упит спрема серверот од страна на корисникот на веб сервис. Корисникот привидно мисли дека комуницира со веб сервисот преку интернет, интранет или друга компјутерска мрежа, а реалноста е дека тој комуницира со „proxy“ класата, која е локална на корисникот. „Proxy“ класата има задача да ги изврши сите комуникациски поединости потребни за праќање на податоци преку интернет до серверот. Исто така „proxy“ класата ги прима резултатите и ги презентира на корисникот. Ова е возможно доколку претходно е исполнет условот дека „proxy“ класата е регистрирана од корисничката апликација.



Слика 12. Принцип на работа на веб сервисот

4.4 Модел на решение за интеграција на сервисно-ориентирани информациски системи со ИСР

Интеграцијата на информациските системи е важна поради комплексноста на процесите кои се одвиваат во разузнвањето, но исто така интегрирањето на информациските системи има значајно влијание и во другите сфери на општеството.

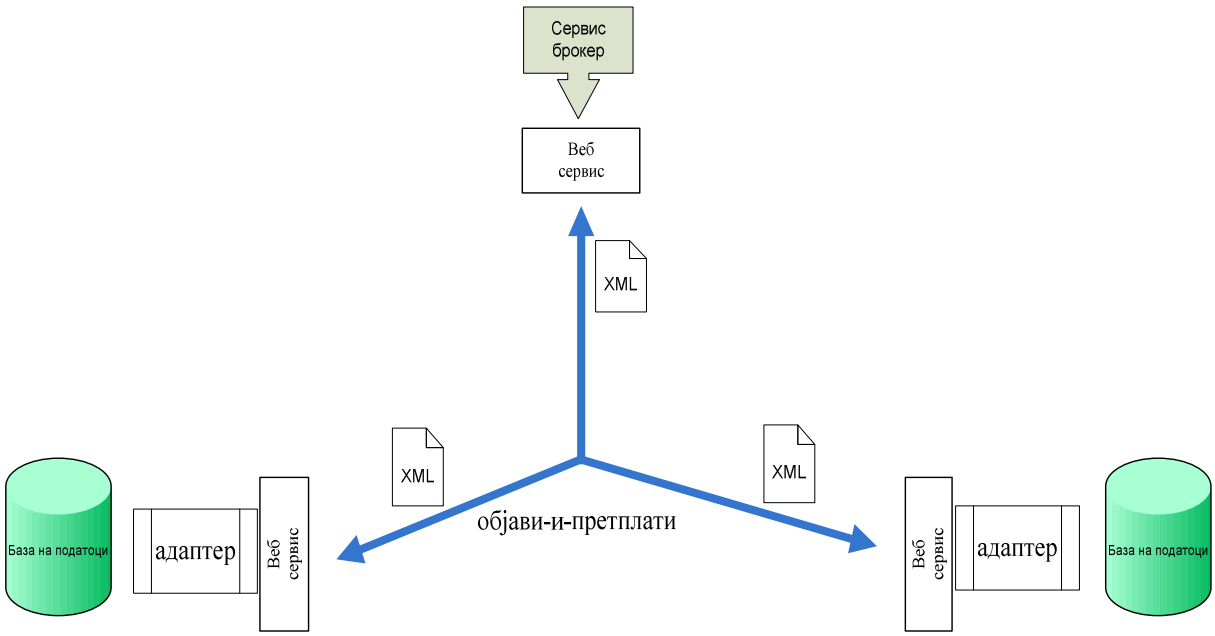
Постоечките модели за интеграција на информациските системи имаат ограничувања во однос на сигурноста на системите, потоа нивната стабилност и воспоставената комуникација во реално време. Веб сервисите се можно решение за надминување на интеграциските проблеми ([6]). Информациските системи може да се интегрираат со различни веб сервиси, во зависностод функцијата и намената. Веб сервисите се презентирани со „WSDL“, преку кој се опишува комуникацискиот интерфејс ([11]).

Употребата на веб сервиси во сервисно ориентираната архитектура е решение кое се предлага за интеграција на информациските системи ([17]). Со користење на наведената архитектура, во текот на дизајнирање, тестирање и користење на информацискиот систем, инженерите нема потреба да навлегуваат во софтверските апликации, кои се користат за интегрирање во информациските системи. Најважно е разбирањето на комуникацискиот

интерфејс за секој веб сервис. Веб сервисите се очекува да бидат користени во интеграција со информациските системи преку методот на поврзување „peer-to-peer“.

Интеграција на бизнис апликациите (*engl.* Enterprise Aplication Integration (EAI)) најчесто означува збир на технологии кои овозможуваат интероперабилност на посебните информациски системи. Главната примена на концептот се темели на интеграцијата на разноразните бизнис апликации и автоматизација на процесите, така што сервисно орентираната архитектура претставува главна основа за конкретните апликациски интегративни решенија ([4]). Под интеграција на апликациите се подразбира изградба на систем составен од софтверски компоненти кои меѓусебно комуницираат преку стандардизирани пораки. Одредени компоненти од тој систем се нарекуваат адаптери при што истите ги користат „надворешните“ компоненти кои е потребно да се интегрираат во системот.

Адаптерите им овозможуваат на надворешните компоненти потполна изолација од потребата за познавање на внатрешната логика на бизнис процесите во кои учествуваат и интегрираните бизнис системи, при што се обезбедува висока интеграциона флексибилност. Пораките најчесто се разменуваат по принципот објави-и-претплати (*engl.* publish-and-subscribe) при што обично постои одредена централна компонента (Слика 13) (*engl.*broker), чија задача е примање и распределба на пораките во системот. Адаптерските и останатите компоненти на системот може да се „претплатат“ на одреден тип на пораки, а брокерската компонента по приемот на секоја порака, им ја проследува истата на сите претплатени примачи.



Слика 13. Адаптер по модел на интеграција со hub/spoke ([19])

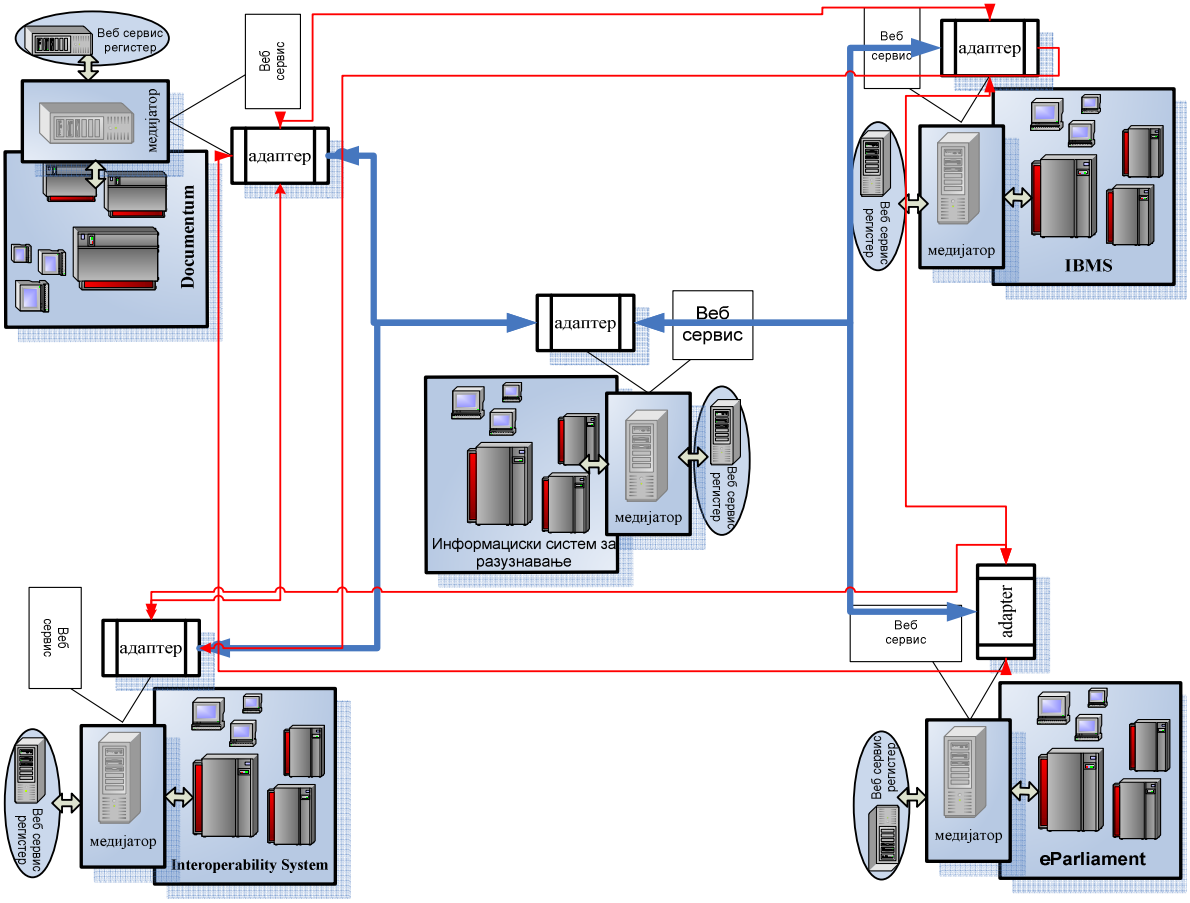
Исто така, возможна е и поедноставна архитектура каде примателот и испраќачот директно комуницираат преку пораки, но моделот објави-и-претплати овозможува поголема флексибилност и отвореност на системите.

Архитектурата во која примателот и испраќачот комуницираат преку пораки е возможна и со „messaging backbone (bus)“. Апликациите ги објавуваат своите пораки

преку „messaging backbone (bus)“ со употреба на адаптери. Пораките ќе го користат „bus“-от за да ги пронајдат претплатените апликации. Претплатените апликации имаат адаптери кои ги препознаваат пораките од „bus“-от, при што ќе ги трансформираат пораките во формат препознатлив за самите апликации. Клучна разлика помеѓу брокерската архитектура која користи „hub/spoke“ топологија и „bus“ топологијата се состои во тоа што интеграцискака компонента која го изведува трансформирањето на пораките и нивното насочување е дистрибуирана во апликациските адаптери, при што исто така bus архитектурата побарува апликациските адаптери да користат иста платформа како и оргиналните апликации ([2]).

Пораките кои се разменуваат мора да бидат стандардизирани внатре во системот за да се олесни интеграцијата. Адаптерите кои претставуваат главни точки на контакт со надворшниот свет, поседуваат трансфомациска логика за трансформирање на стандардните пораки во формат во кој надворешните апликации го очекуваат. Во најголем број на случаи „XML“ технологијата е подобна за имплементација на стандардните пораки, при што со „XML shema“ се постигнува дефиниција и рестрикција на типовите на пораки кои се разменуваат во системите. Начинот на размена во системите се постигнува преку стандардизиран интефејс по пат на утврдени протоколи. Едно од најдобрите решенија е користење на протоколи како „HTTP/SOAP“, со интефејси кои се базираат на технологија на веб сервиси.

На Слика 14 подолу е решение за интеграција на информациски системи со информацискиот систем за разузнавање ([18]).



Слика 14. Поврзување на информациски системи со ИСР преку веб сервиси (*engl.* peer-to-peer)

Корисничките функционалности на системот можат да се третираат од повеќе аспекти согласно со поделбата на корисници. Како што веќе беше елаборирано, постојат четири видови на крајни корисници на ИСР. Тоа се:

- Корисник на сервиси
- Сервис провајдер
- Компании
- Разузнавање (IMINT, SIGINT, OSINT, MASINT)

Со анализа на процесите кои треба да постојат во институциите вклучени во ИСР, може да се заклучи дека крајните корисници можат да користат исто мета корисничко сценарио, односно секогаш да работат по иста генерална процедура (процес). Тој процес е составен од три фази (подпроцеси). Тие фази се:

- фаза на евиденција,
- фаза на верификација,
- фаза на нотификација.

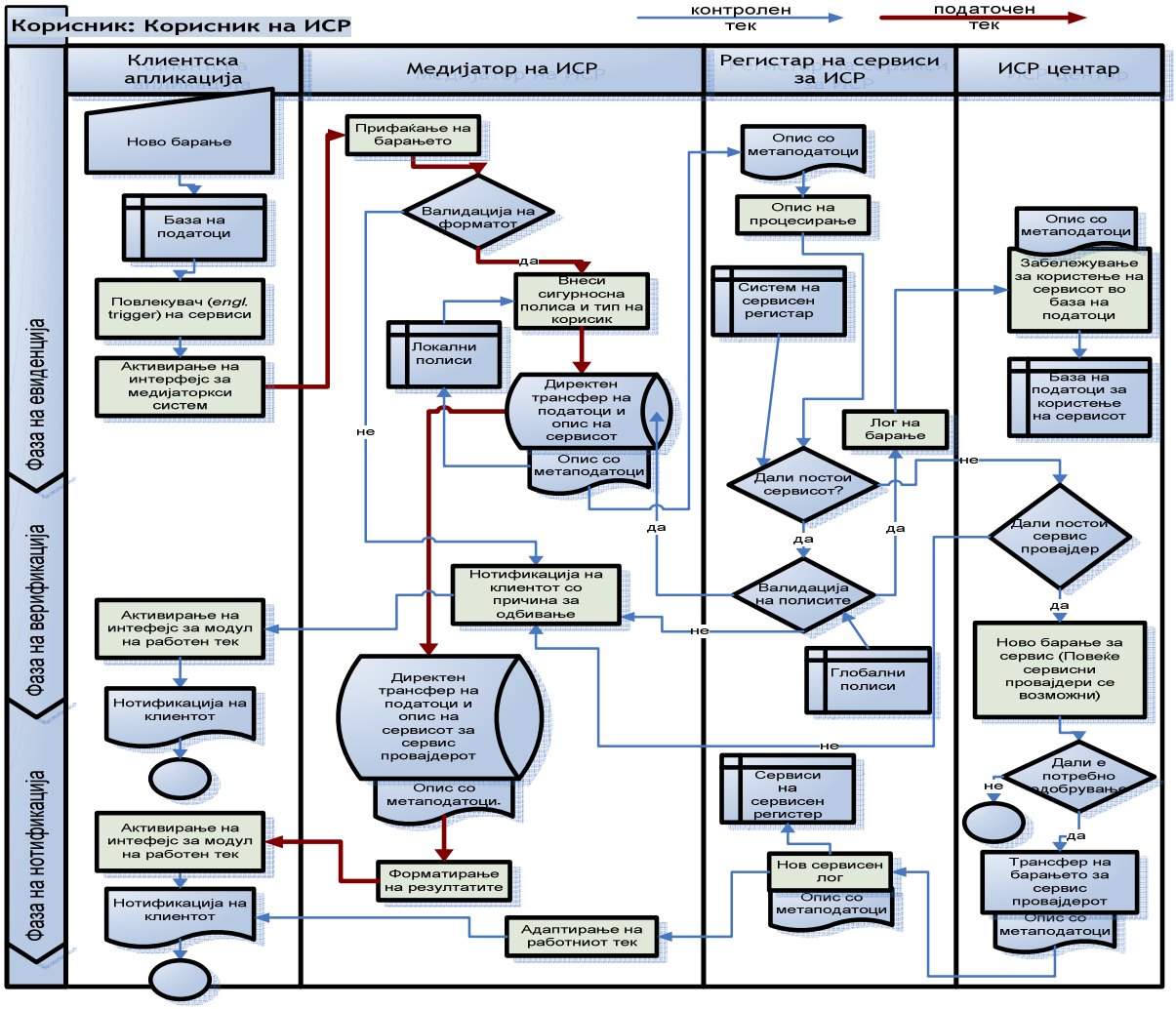
Овие фази постојат во секој процес поврзан на ИСР, но не секогаш се предмет на подршка на ИСР. Понекогаш се поддржани од интерните информациски системи на институциите вклучени во процесот на ИСР. Тоа е дополнителна причина за потреба од интегрирање на систем за поддршка workflow на медијаторско ниво во сите институции вклучени во процесот на разузнавање.

Графичкиот тек на податоците на контрола и корисните податоци за услугата е претставен на Слика 15. На истата слика се гледа како се разменуваат сите податоци помеѓу главните модули на ИСР: клиентска апликација во институција вклучена во процесот на разузнавање, медијаторскиот модул на ИСР, системот на сервисни регистри, и информацискиот систем за центарот за разузнавање. На сликата се назначени и фазите на генералниот процес.

Битно е да се напомене дека истата слика опишува и побарување услуга, и давање одговор на побарана услуга. И во двата случаи, клиентската апликација треба да добие нотификација преку обезбедениот интерфејс. Од дијаграмот се гледа дека:

- постои евиденција на секое барање на услуга;
- постои евиденција на секое искористување на услуга;
- услугата се извршува само ако соодветните локални и глобални полиси го дозволуваат тоа;
- корисничките информации се разменуваат само на ниво на медијатори кои во себе интегрираат полиси, трансакции и реформатирање (види Архитектура на ИСР);
- доколку некоја услуга не постои, но се добие валиден формат за барање, тоа барање ќе се евидентира, и доколку постои соодветен обезбедувач на услуги, неговиот медијаторски систем ќе треба да ја обезбеди истата. Во тој процес новата услуга се евидентира во регистерот на расположиви услуги;

Генералната корисничка итерација може да се преслика во поспецифични кориснички функционалности на сите четири типа на крајни корисници. Тоа ќе биде претставено со глобалните кориснички функционалности за четирите типови на крајни корисници.



Слика 15. Претставување на генералната корисничка итерација на крајниот корисник на ИСР

Сервис провајдер. Фазата на дефинирање на услуга/правило опфаќа:

- дефинирање на тек на работа (*engl.* workflow) за бараниот сервис со помош на графички едитор, при што се одредуваат актерите во процесот, нивните привилегии и обврски;
- дефинирање на форматот на податоците (пример „SOAP“ во случај на веб сервиси) и принципот на нивната размена преку соодветна спецификација (пример „WSDL“ во случај на веб сервиси);
- дефинирање на степенот на достапност на услугата (дали треба да е достапна преку интернет, интранет или одделна мрежа);
- публикување на услугата во соодветен јавен, интерен или приватен регистар на услуги („UDDI“ во случај на веб сервиси).

Фазата на периодична валидација на услуга/правило опфаќа:

- проверка на правилата на пристап на услугата при секоја промена на интерните правила на службите и при секоја законска промена. По потреба стопирање на услугата (при што се врши автоматско известување на нејзините корисници);

- ажурирање на правилата за користење на услугата (на ниво на процес, не на ниво на формат на податоци). Во случај на потреба од промена на форматот на податоците, услугата се стопира (при што се врши автоматско известување на нејзините корисници) и се дефинира нова услуга;
- воведување на дополнителни процеси на филтрирање на содржините на информациите доколку е потребно.

Фазата на активирање на услуга/правило опфаќа:

- публикување на услугата во соодветен јавен, интерен или приватен регистар на услуги („UDDI“ во случај на веб сервиси).

Корисник на сервиси. Фазата на барање на услуга опфаќа:

- пребарување на расположиви услуги низ регистрите на услуги (во зависност од дефинираното право на пристап, барателот ќе може да ги пребарува интернет, интранет и одделните регистри на услуги);
- доколку услугата веќе не е дефинирана (одобрена) се праќа барање за услуга до центарот за разузнавање со проследена спецификација за форматот на податоците (пример „SOAP“ во случај на веб сервис).

Фазата на валидација на услугата опфаќа:

- центарот за разузнавање одредува кој е одговорен за информациите и го препраќа барањето до соодветниот одобрувач на услуги, по што се активира корисничкото сценарио на одобрувач на услуги.

Фазата на користење на услугата опфаќа:

- активно користење на услугата, кое се евидентира во системот;
- добивање на информации за стопирање или промена на достапноста на информации поврзани со услугата;
- добивање периодични извештаи и извештаи по барање за користењето на услугата за потребите на системите за внатрешна контрола;
- можност за давање на мислење (оцена) за квалитетот на услугата до обезбедувачот на услугата.

Разузнавање. Фазата на идентификацијата и верификацијата опфаќа:

- идентификација на лица, врз основа на воочена потреба (на пример: следење на лица);
- идентификација на борбени средства и вооружување и нивна верификација врз основа на дигитална информација или официјален документ, со можност за автоматска детекција
- идентификација на добра и нивна верификација.

Фазата на контрола опфаќа:

- споредба на верификуваните информации од претходната фаза со информации од различни извори (внатрешни и надворешни) кои можат да бидат менливи во текот на времето, а со цел да се открие сомнителен настан или сторено дело.

Фазата на налози и проследувања опфаќа:

- автоматско евидентирање на настани кои можат откако ќе бидат одобрени од множество на активни автоматски и мануелни полиси да обезбедат извори на информации на институциите вклучени во процесот на разузнавање.

Компании. Фазата на идентификацијата и верификацијата опфаќа:

- пополнување на електронски формулари.

Фазата на контрола опфаќа:

- проверка на информациите по однос на барањето, одобрување на барањето.

Фазата на проверка на статус опфаќа:

- давање на информација за статусот на барањето.

Како што се гледа од елаборацијата, кај сите типови крајни корисници, фазите на генералниот процес на функционалност на ИСР постојат, а поделбата на типови корисници е всушност извршена согласно примената на сигурносните полиси и предметот на поделба на функционалностите од фазите (дали се предмет на реализација на ИСР или се предмет на реализација кој треба да е покриен од информациските системи на одделните институции вклучени во процесот на разузнавање).

Следните кориснички сценарија се дадени како пример на специфични функционалности кој ИСР може да ги обезбеди за крајните корисници.

Избрани се пример кориснички сценарија кои содржат карактеристични случаи со кои треба да се соочи ИСР. Такви сценарија се сценарија кои:

- обезбедуваат информации од една институција, но од повеќе извори на податоци. Сценарија кои повикуваат други сценарија или самите себеси или пак се повикуваат во итерација;
- сценарија кои побаруваат координација на работа на повеќе институции;
- сценарија кои обезбедуваат поддршка на специфични барања на одредена институција.

ГЛАВА 5

ПРЕГЛЕД НА СИГУРНОСНИ РЕШЕНИЈА ЗА СЕРВИСНО ОРИЕНТИРАН ИНФОРМАЦИСКИ СИСТЕМ ЗА РАЗУЗНАВАЊЕ

Сигурноста е многу важен предуслов во сервисно ориентираната архитектура, бидејќи СОА содржи сервиси имплентирани на различни оперативни платформи и распространети на различни локации. Главниот предизвик за СОА сигурноста „лебди во облаци“, а тоа се однесува на недоволно креираната рамка за сигурносни модели базирана на постојани и соодветни методи.

Во поглавјето е предложено сигурносно решение за информациски систем за разузнавање целосно базиран на СОА. Современите безбедносни архитектури и бездносни протоколи се во фаза на развој. СОА базираните системи се карактеризираат со разлики во сигурносната имплментација и тоа според контрола на пристапот (*engl.* access control), сигурносниот менаџмент (*engl.* security management) во различни домени, потоа шифрирање (*engl.* encryption), сигурносен мониторинг (*engl.* security monitoring) итн. Домените како крајни точки имаат сервиси во информациските системи кои вообичаено формираат композитни сервиси. Процесот кој е воспоставен со композитните сервиси е проширен на различни крајни точки во различни домени.

Целта на поглавјето се однесува на разработување соодветно сигурносно решение за информацискиот систем за разузнавање со употреба на сигурносните стандарди за веб сервисите, сè со цел да се достигне одредено ниво информациска сигурност како автентификација, авторизација, интегритет, приватност, федеративен идентитет и други.

Во поглавјето е прикажано решение во кое информациите обезбедени од сервисите се препраќаат од креаторите на информациите до корисниците на информациите. Воведен е сигурносен и логирачки ситем (*engl.* security and loging system), кој ќе се користи како слој посредник за верификација и валидација (*engl.*verification and validation middleware).

За да се постигне претходно наведеното, сервисно-ориентираните информациски системи е потребно да ги исполнуваат сигурносните барања и цели на ниво утврдено според претходно дефинирани стандарди, за време на процесот на нивното креирање и планирање.

Поглавјето е поделено во неколку секции и тоа: во првата секција се презентирани сигурносните решенија за заштита на СОА базираните системи. Целите кои треба да се постигна со СОА сигурноста (*engl.* SOA Security) се презентирани во втората секцијата. Третата секцијата содржи опис на почесто користените сигурносни протоколи за веб сервиси како „XML“, „XML encryption“, „XML signature“, „SAML“, „SOAP“ и други стандарди во рамките на „WS-Security“. Моделот за сигурносното решение за сервисно ориентираниот информациски систем за разузнавање и неговата имплементација е презентиран во четвртата секцијата.

5.1 Преглед на истражувања за сигурност за информациски системи базирани на СОА

Во ([78]), авторите проектирале дека 90% од надворешните напади на апликациите се однесуваат на сигурносните пропусти и неконфигурираните системи. Бидејќи не е возможно да се развие 100% сигурносна апликација, најсоодветно е да се анализираат заканите, пропустите, ризиците, со цел да се креираат сигурносни механизми како решение за СОА базираните системи. На овој начин, дефинираните сигурносни решенија ја подобруваат сигурноста во целиот систем и придонесуваат во намалување на трошоците при справување со инцидентите, трошоци за оporавување, трошоци за намалување на репутацијата итн. Исто така во истражувањето се дадени насоки за имплементирање на сигурносните решенија и нивна интеграција како и имплементирање на контрола на пристапот согласно СОА иницијативите. Во истражувањето се разработени следните секции: Модели за контрола на пристап, Мета-модел за СОА на веб (*engl.* Web service-oriented architecture (WSOA)), Цели на сигурносните решенија за СОА, Модели за имплементација на сигурносните решенија за СОА, Индустриски стандарди за СОА сигурност и сервисно-оринтирана информациска интеграција (*engl.* Service-Oriented Information Integration (SOII))

Во ([79]) е објаснето дека осигурувањето на сервисно-ориентираните системи е предизвик, бидејќи сигурносните сервиси (*engl.* security services) се еднакво дистрибуирани како и сервисите за работните процеси (*engl.*workflow services) во СОА базираните системи. Воспоставувањето на сигурност само на крајните точки не е адекватно решение за СОА системите. Од друга страна, имплементирањето на сигурносни сервиси на секоја крајна точка предизвикува големи финасиски импликации. Моментално, постојат скромни истражувања за одвојување на сигурноста од крајните сервисни точки. Како решение е даден моделот „Security As A Service (SAAS)“, кој ги надминува сигурносните граници на крајните точки на системот, преку користење на споделени сигурносни сервиси во рамките на сигурносниот домен. Сигурносните сервиси се составени од интегрирани компоненти базирани на моделите како „Service Component Architecture (SCA)“. Во истражувањето „SAAS“ парадигмата е разработена како решение за осигурување на „SECTISSIMO“ платформата. Исто така, во истражувањето е презентирана референтна сигурносна архитектура за осигурување на критичните СОА системи базирани на парадигмата „SAAS“.

Во ([80]), авторите го воведуваат „SAAS“ пристапот и предлагаат сервис за сигурносно одлучување (*engl.* Security Decision Service (SDS)), со кое обезбедува сервисно-базирани „Policy Decision Points (PDP)“ на различни извршни точки.

Посеопфатно решение е дадено во ([81]), каде се имплементираат автентификацијата, довербата (*engl.* trust) и сигурносната конверзација (*engl.* secure conversation), како посебни сервиси за да се разрешат проблемите со сигурносниот менаџмент и интероперабилните проблеми.

Во ([82]), авторот презентира преглед на специфичните решенија за сигурноста во SOS архитектури.

5.2 Сигурност и контрола на пристап

Разработувањето на концептот за СОА сигурност дава до знаење дека е потребно да се разбере сигурноста од различни аспекти, потоа улогата на „AAA (Authentication,

Authorization и Auditing)“ во СОА сигурноста и нивната имплементација како индустриски стандарди. Особено внимение треба да биде посветено на сигурноста на веб сервисите (*engl.* web service security), бидејќи веб сервисите се искористени во имплементирањето на СОА парадигмата ([78]).

Со зголеменото користење на СОА, границите за користење на сервисите се намалуваат, при што неограниченото користење на апликациите без зависност од платформата и софтверот претставува сеопфатно решение. Со цел да се постигне вистинска повторна употребливост на сервисите (*engl.* reusability of services), потребно е организациите да овозможат пристап на трети страни, партнери и други крајни корисници низ несигурна компјутерска мрежа како Интернет. Сервисите се организациски имот, така да е потребно да бидат превземени одредени безбедносни мерки, бидејќи со неправилни мерки на безбедност нивото на закана за организациите ([85]) се зголемува во форма на неавторизиран пристап, хакерски напади, погрешно користење на сервисите и прекумерно користење на сервисите.

Сигурносните системи потребно е да овозможат бизнис апликациите да ги исполнат неопходните кориснички барања, со цел да се постигнат сигурносните цели: автентификација, авторизација, федеративен идентитет, приватност, интегритет, достапност, неможност за одрекување во смисол на пратени и примени пораки од корисниците.

Автентификација ([83]) претставува проверка на идентитот на субјектот. Субјект може да биде корисник, веб сервис, компјутер или апликација. Автентификацијата е прв чекор во контрола на правата на пристап. Со цел да се овозможи контрола на правата на пристап на одредено ниво, потребно е системот да ги идентификува субјектите и при тоа да има соодветно ниво на доверба во автентичноста на идентитетот на субјектот. Заедничката автентификација помеѓу актерите претставува двосмерна автентификација и дозволува доверба на идетитетот на двете страни вклучени во комуникацијата.

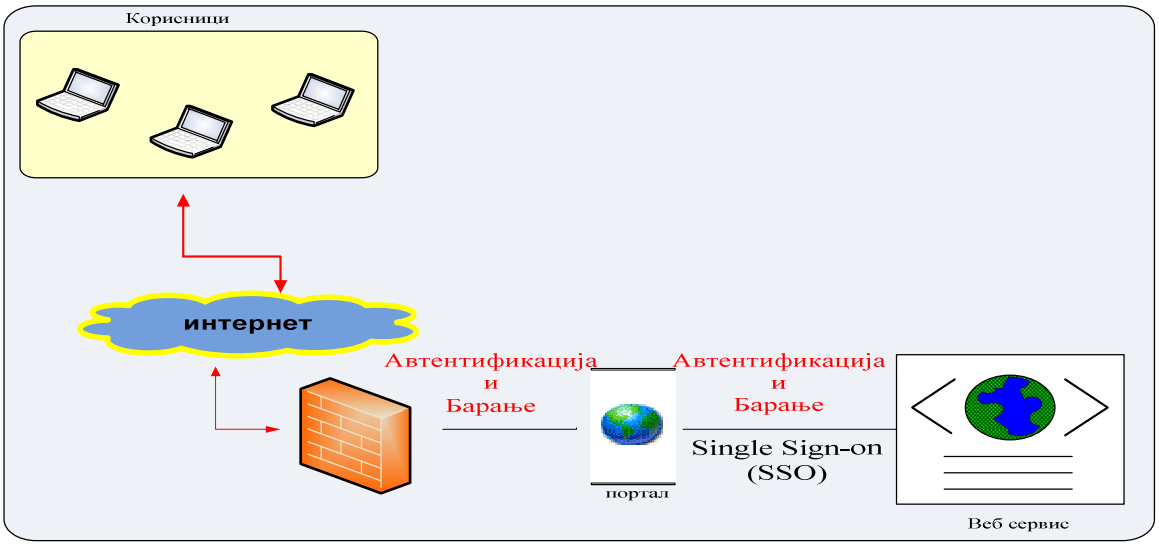
Постојат различни механизми за автентификација, но најкористе се следните:

- корисничко име и лозинка;
- дигитален сертификат;
- биометриски уреди.

Протоколи кои се користат за енкрипција се следните: „SSL/TLS“ (Secure Sockets Layer)/ (Transport Layer Security). Овие протоколи имаат вметнато механизми за автентификација за проверка на корисничкото име и лозинката и проверка на дигиталниот сертификат. Без разлика на нивото на сигурност, наведениот протокол може да се користи за проверка на автентификација на само два субјекти истовремено. Најважно е последната компонента од процесот да го прифати идентитетот на иницијалната компонента односно корисникот, што подразбира дека СОА базираните системи може да користат „SSL“ протоколи, но истовремено треба да бидат надоградени со други безбедносни механизми.

Слика 16 претставува пример на корисник кој се автентифицира на портал и праќа барање за користење на сервис. Во примерот е употребена метода наречена „sender-vouch“, што означува дека порталот гарантира за идентитетот на корисникот. Ова е една од методите за пренесување на идентитетот (*engl.*identity propagation) и истата се користи во „Web Service Security“ (WS-S). Употребата на методот наречен „Single sign-on“ (SSO) дозволува пренесување на идентитетот на апликациите и сервисите. Порталот треба да обезбеди виско ниво на гаранција со цел да се воспостави доверба меѓу сервисите и корисниците. Тоа значи дека сервисите треба да веруваат во автентификацијата на

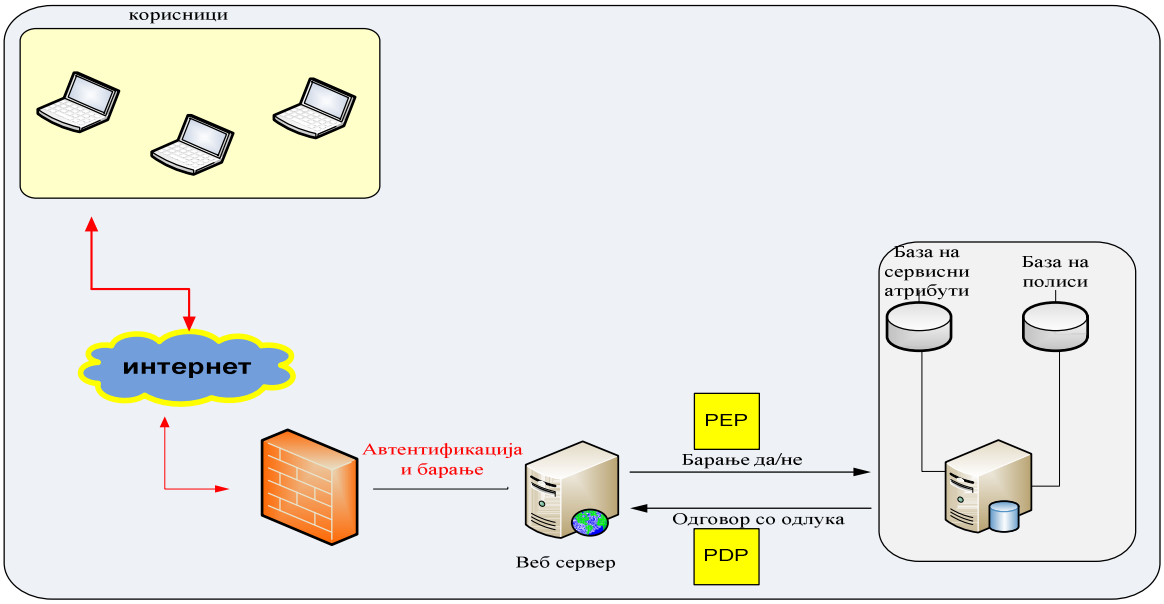
порталот и неговата точност, бидејќи тој ги дава гарнциите. Двата типова на доверба потребно е да се разработуваат посебно ([83]).



Слика 16. Пример за пренесување на идентитетот (*engl.*identity propagation)

Авторизација ([83], [88]) претставува одредување на правото на пристап и дозвола која корисникот ја поседува. По завршување на процесот на автентификација и проверка на идентитетот, системот ги одредува правата за пристап на корисникот и ресурсите кои се дозволени за употреба на корисникот.

Флексибилност во авторизација може да се постигне со креирање на точка за одлучување на правото на пристап (*engl.* Policy Decision Points (PDP)) и точка која ги извршува (*engl.* Policy Enforcement Points (PEP)) одлуките од „PDP“ кои се однесуваат на корисникот (Слика 17).



Слика 17. Употреба на PEP/ PDP процесот на авторизација

Авторизацијата може да се подели на два типа на контрола на пристап:

- Дискретна контрола на пристап (*engl.* Discretionary Access Control (DAC))
- Задолжителна контрола на пристап (*engl.* Mandatory Access Control (MAC))

„DAC“ ја забранува контролата на пристап базирана на дозвола, права, атрибути и групи каде субјектот припаѓа. Дозволата за користење на ресурсите на системот е централизирана, односно субјектот побарува пристап, а „PDP“ одлучува за правото на пристап. Наведениот тип на авторизација, генерално се употребува во комерцијалните COA базирани информациски системи.

„MAC“ типот на авторизација, генерално е употребен во владините COA базирани информациски системи, при што преку него се контролираат правата на пристап кои се однесуваат на сигурносните дозволи и сигурносните симболи на ресурсите. Тоа значи дека податоците треба да имаат сигурносни симболи и „PEP“ точките мора да го детерминираат корисничките права на пристап, а исто така и побаруваните ресурси на начин на правење споредба помеѓу сигурносните симболи и одобрените права на пристап на субјектот.

Контрола на пристап базирана на улога (*engl.* Role –Based Access Control (RBAC)) е вообичаена метода користена во дискретна контрола на пристап. Сигурносните улоги се одредени за субјектот, а правото за користење на ресурсите е дефинирано со сигурносните улоги. Врз основа на корисничките права и улогите на субјектот, „PDP“ одлучува за правото на пристап.

Контрола на пристап базирана на атрибутите (*engl.*Attribute-Based access Control (ABAC)) е слична метода на „RBAC“, а разликата во методите е дека во „ABAC“ се користат сигурнисните атрибути наместо сигурносните улоги. Во таков систем, атрибутите за авторизација се претставени со улоги, групи и сигурносни одобрување. Контролата на пристап базирана на атрибутите е искористена во методите за дискретната и задолжителната контрола на пристап.

Контрола на пристап базирана на однапред одредена авторизациска одлука (*engl.* Predetermined Authorization Decision-Based Access Control (PADBAC)) е метода за контрола на пристап која ги користи „MAC“ и „DAC“ методите за контрола на правота на пристап. Карактеристично за оваа метода е дека корисничките права се презентирани во облик на карти и истите ќе бидат употребени во за пристап до ресурсите.

Федеративен идентитет ([83]) е наменет да им овозможи на корисниците да пристапат на повеќе сигурносни домени со користење на една идентификација. Сигурносните домени се компоненти во различни компании кои имаат сопствени ресурси. Множевството на партнерски компании се нарекува федерација и корисниците може да пристапуваат на различни точки во домените со користење на „Single sign-on“ (SSO) методот. Исто така, методот за пристап во федеративниот идентитет е поделен преку проценка на методите валидација и авторизација. Врз основа на претходно наведеното, потребно е компаниите да „веруваат“ на надворешните идентите, при што не е потребно да креираат сопствени локани идентитети за секој субјект посебно, кој пристапува како надворешен корисник со цел да ги употреби ресурсите на компанијата. Сигурносниот тип на пристап ги намалува трошоците на компаниите за менаџирање со системите со сигурност, без да се предизвикаат негативни импликации по безбедноста.

Успешноста на системот за федеративен идентитет зависи од способностите за делење на заедничкото множество барања помеѓу компаниите. Идејата за федеративен

идентитет евалуира, така што покрај идентитетот го проширува своето влијание на други информации. Постојат два протокола за пристап во федеративна околина:

- Протокол на „SSO“ базиран на пребарувач (*engl.* Browser-based SSO), кој се употребува од пребарувачот на клиентот и веб апликацијата со користење на „Hypertext Transfer Protocol“ (HTTP);
- Протокол на „SSO“ базиран базиран на сервис (*engl.* Service-based SSO), кој се користи помеѓу два сервиси.

Динамичките релации се многу важна карактеристика на федералниот идентитет. Иако, федеративниот идентитет е долгорочно решение, барањата за флексибилен модел во динамичната бизнис околина се поважни во современо општество. Сите актери кои се дел од воспоставената архитектура потребно е да креираат силна координација помеѓу бизнис процесите. Исто така се доста важен сегмент заштита на приватноста и доверливоста на информациите.

Во 2005 година Организацијата „OASIS“ (*engl.*Organization for the Advancement of Structured Information Standards) го публикуваше стандардот „SAML 2.0“ (*engl.* Security Assertion Markup Language), кој се однесува на федеративниот идентитет. Организацијата „The Liberty Alliance“ го има публикувано стандардот „ID-WSF“ (Identity Web Services Framework) кој е базиран на „SAML 2.0“. Наведените два стандарди се најмногу користени во моделот за федеративен идентитет.

Приватност ([83]) претставува тек на информациите низ сигурносна околина, при што потребно е секоја комуникација воспоставена помеѓу авторизирани учесници да биде заштитена особено во сегментот на приватноста на информацијата. Приватноста се постигнува со енкрипција на сензитивни информации. Во процесот на енкрипција вообичаените текстуални пораки се енкриптираат со употреба на алгоритми за криптозаштита и како резултат од страна на примателот на пораката примена е криптирана порака. Постојат различни алгоритми за криптозаштита, но најчесто користени се симетрични алгоритми кои користат таен клуч и асиметрични алгоритми кои користат јавен клуч.

Во СОА бизнис околина ([86]) може да користат и класифицирани информации, но за тоа е потребно постигнување на соодветно ниво на енкрипција. Различните протоколи даваат можност за масовна енкрипција (*engl.* bulk encryption) помеѓу две точки. Но, како и да е, употребата на овие протоколи е ограничена бидејќи некои СОА системи не дозволуваат масовна енкрипција. Претходнонаведените протоколи дозволуваат заштитена комуникација единствено помеѓу две точки, но секоја точка која се наоѓа на патеката помеѓу праќачот и примателот на пораката ќе може да ја користи информацијата. Во наведените протоколи исто така е „SSL/TLS“ протоколот.

Во креирање на решение за постигнување на приватност потребно е да опфати следното:

- менаџирање со клучеви – начин на дистрибуирање на клучевите;
- избор на шифри;
- криптографски протоколи кои ги обезбедуваат сервисите;
- одредување на ниво на енкрипција потребно да се постигне сигурносните барања на компанијата.

Користењето на тајните клучеви за енкрипција на информациите е предизвик. Криптографијата со јавен клуч се употребува во проверување на тајните клучеви кои се користат за енкрипција.

Стандардите како „SSL“, дозволуваат користење на клучеви за сесии кои се однесуваат на долгорочните сесии како „HTTP“. Пораките се разменуваат помеѓу двете страни со користење на еквивалентен клуч, при што се обезбедува приватност на пораките за времетраењето на сесијата.

Стандардите како што е „WS-Security SOAP messaging“ ([83], [87]) немаат подршка за концептот со сесии и истите се проблематични кога е неопходно да се воспостави долгорочна размена на порака. Ова е последица на тоа што е неопходно за секоја порака да се изврши преговарање односно енкрипција со јавен клуч за да се утврди веродостојноста на тајниот клуч. Како резултат се појавува комбинацијата од „WS-Security SOAP messaging“ и „SSL“ стандардот помеѓу две точки за комуникација. Во 2007 год. „OASIS“ ([90]) го пропишува стандардот под назив „WS-SecureConversation“ кој се користи за воспоставување на долгорочни сесии со користење на „WS-trust“ моделот.

Интегритет ([83]). Во комуникацијата, а посебно во сервисните трансакции, потребно е воспоставување на контрола во однос на проверка дали податоците се фалсификувани или менувани на било кој начин. Валидноста на интегритетот на податоците претставува технологија на докажување дали пораката е менувана од страна на неавторизиран субјект. Заради можноста од злоупотреба на пораките од кои поминуваат низ „TCP/IP“ мрежите, потребно е да се користат дигитални потписи, автентификациони кодови или хаш алгоритми за да се потврди валидноста на интегритетот на пораката.

Во СОА околина потребни се механизми, кои ќе обезбедат валидност на интегритетот на пораката, помеѓу секој корисник на сервис и провајдер на сервис. Примачот на пораката мора да има високо ниво на уверување дека таа не е изменета од страна на некој што не е учесник во комуникацијата. Покрај тоа потребно е примачот да има доверба дека пораката со валиден интегритет не е реплицирана од трета страна која може да ја злоупотреби. Од оваа причина, безбедносните протоколи за пораки користат механизми за интегритет за комбинирање на пораките со временски ознаки и идентификатори за пораките. На овој начин се гарантира датумот, времето, идентитетот и самата порака. Ако интегритетот на временската ознака или идентитетот на пораката не е валиден или ако временската ознака истекла или ако е пораката менувана и ако е пораката пратена со иста идентификација тогаш примачот автоматски ја одбива. Механизмите кои „WS-Security SOAP messaging“ спецификацијата ги дозволува обезбедуваат интегритет на пораката покрај можноста за спречување на напади на повторно пратени пораки.

„SSL/TLS“ протоколот обезбедува интегритет помеѓу две точки, комбинирајќи ги со механизмите за автентификација и доверливост. Сепак наведениот протокол не дозволува соодветно ниво на заштита во СОА системите.

„XML signature“ стандардот е пропишан од „W3C“, при што истиот се користи како дел од решение на претходниот проблем. Оригиналното барање е дигитално потпишано и така се пренесува понатаму. На тој начин се обезбедува интегритетот на пораката. Доколку податокот се измени во било кој момент, проверката за интегритетот ќе биде негативна. Притоа, истовремено се користи и „XML“ потписот за да се спречи повторното праќање на истата порака.

Како заклучок може да се наведе дека најдобро решение, по прашање на безбедноста во рамките на СОА околина во однос на интегритетот, е разработување на сите сценарија за користење на сервисите.

Неможност за одрекување (*engl.* Non-repudiation) ([83]) е последица на дигиталното потпишување на пораката и претставува легален доказ дека субјектот ја потпишал пораката. Дигиталниот потпис криптографски ги поврзува идентитетот на потпишувачот со содржината на потпишаната порака. Користењето на криптографијата со јавен клуч овозможува неотповикливост на праќачот на пораката дека тој ја потпишал истата.

Користењето на „XML Signature“ стандардот за потпишување на пораките или само поедини делови на пораката, овозможува докажување на интегритетот и неможност за одрекување на потписот. Наведениот стандард може да се користи со сервисите кои се базираат на „REST“ и „WS-Security SOAP Messaging“ стандардите.

Иако дигиталниот потис дава високо ниво на сигурност важно е дека при имплементација на решенијата за праќање на пораки во рамките на СОА системите потребно е голема претпазливост за постоењето на потенцијалните пропусти и опасностите од примената и користењето на дигиталниот потпис. Голема опасност за нарушување на безбедноста се случува кога одреден „XML“ елемент се потпише без одредување на условите за негово користење или без поврзување со одреден специфичен услов. Во СОА пораките вообичаено е да се нагласат ограничувањата и условите за користење на потпишаните податоци. Кога е потребна идентификација на идентитетот, мора да се изврши криптографско поврзување со конкретен услов со помош на дигиталниот потпис, при што е овозможено користење на потпишаните податоци во други цели. Ова значи дека потписот покрај податоците мора да вклучи и контекст за нивното користење како и временски ограничувања. Постојат разни други опасности при користење на дигиталниот потпис во рамките на СОА. Безбедносните системи кои се базираат на „SOAP“ стандардите претставуваат околина за избегнување на таквите опасности.

5.3 Сигурносни стандарди и спецификација за веб сервиси

„Web services“ и „Web Services Security“ се основаат на голем број на стандарди кои треба да бидат презентирани со цел да се избере соодветно решение за безбедност на инфомациските системи базирани на сервисно ориентираната архитектура.

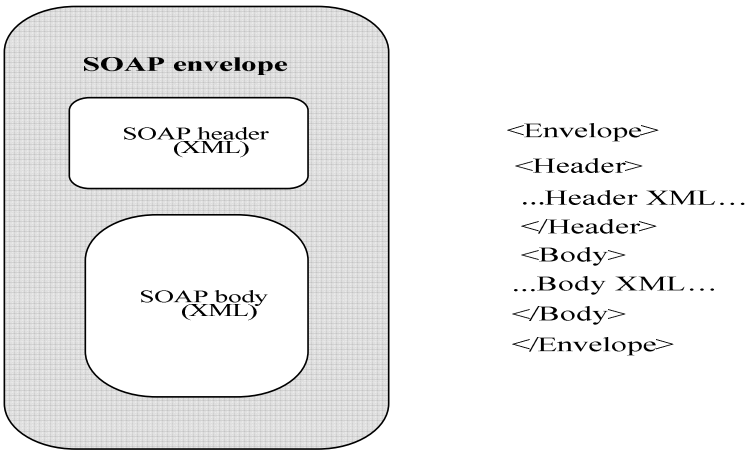
„XML“ (eXtensible Markup Language) е темел врз основа на кој се градат стандардите за веб сервисите и стандардите на безбедност на веб сервисите. „XML“ е отворен стандард одобрен од „World Wide Web Consortium“ (W3C) како метод за размена на податоци со користење на едноставевен текстуален формат. Фактот дека „XML“ е едноставен за читање и можноста за негово користење во хетерогени системи го прави соодветен за веб сервисите и СОА каде сервисот и корисникот може да користат различна платформа.

„SOAP“ (Simple Object Access Protocol) (Слика 18) е важен протокол за пораки кој ја формира основата за протоколите на веб сервисите. „SOAP“ пораките ([84]) се дизајнирани да бидат независни од транспортниот протокол, но се најчесто пренесувани преку„ HTTP“ или „HTTPS“ кога се употребуваат веб сервисите. „SOAP“ пораките не се

цврсто врзани за „HTTP“ протоколот, но тие може да бидат исто така искористени во линија од пораката, пратени преку е-мајл или преку друг транспортен механизам.

„SOAP“ стандардот е базиран на „XML“ и ја дефинира структурата на пораката која треба да помине помеѓу системите. Пораките дефинирани во „SOAP“ имаат плик, заглавие и тело. „SOAP“ заглавието дозволува да се вметнат безбедносни елементи како дигитални потписи и криптозаштита во рамките на пораката. Иако не е ограничено бебзбедносните елементи да се вметнуваат само во заглавието, тие најмногу се користат во „WS-S“ стандардите за заштитено пренесување на информации со пораката.

Постојат два основни модули за пораки користени од „SOAP“ -“document” и повикување од далечина (*engl.* Remote Procedure Call (RPC) mode). Документ модулот е соодветен за еднонасочно пренесување на пораките, во кој корисникот ја праќа пораката, но при тоа не очекува одоговор. „RPC“ модулот е општо употребуван и тоа е барање-одговор модел каде корисникот праќа „SOAP“ барање и потоа очекува „SOAP3 одговор.



Слика 18. Конструкција на „SOAP“ порака ([84])

„XML Signature“ (Слика 19) обезбедува интегритет и автентификација на „XML“ податоците со користење на дигитален потпис и може да се употребува за секоја дигиталилизирана содржина. Основната употреба во рамките на „Web Services Security“ е да го обезбеди интегритетот на потписот на „XML“ пораката и да го докаже идентитетот на потписникот.

```
<Signature ID?
<SignedInfo>
<CanonicalizationMethod/>
<SignatureMethod/>
(<Reference URI? >
 (<Transforms>)?
  <DigestMethod>
  <DigestValue>
</Reference>)+
</SignedInfo>
<SignatureValue>
(<KeyInfo>)?
(<Object ID?>)*
 </Signature>

  ?  =  Zero or More Occurrence
  +   =   One or More Occurrences
  *   =   Zero or More Occurrences
```

Слика 19. Синтакса на неформален „XML signature“ ([84])

„XML Signature“ самостојно се презентира како „XML документ“. Структурата ги содржи следните елементи (Слика 20):

- *„Signature“* содржи елемент кој идентификува дека тоа е дигитален потпис;
- *„SignedInfo“* содржи референци за податоците и одредува дека се дигитално потпишани
- *„CanonicalizationMethod“* се однесува на начинот на кој „SignedInfo“ елементот се подготвува пред потписот да се калкулира. Причината за ова е дека различни платформи може да ги интепретираа податоците малку поразлично (e.g., carriage returns <CR> versus carriage return/line feeds <CRLF>), при што може да предизвика потписот да се програмира различно на различни платформи.
- *„SignatureMethod“* се однесува на алгоритмот употребен за создавање или валидација на потписот, како на пример *„dsa-sha1“* кој се однесува на употребата на „DSA“ алгоритмот со „SHA-1“ функцијата за хаширање;
- *„Reference“* елементот е комплексен, но најважно е дека истиот се однесува на податок кој треба да е потпишани и истиот е дел од „XML“ податоците или од „Uniform Resource Identifier“ (URI) кој се однесува на надворешните податоци како документ, веб страна или друга дигитлана содржина. Во продолжение, „Reference“ елементот ги одредеува трансформациите кои ќе имаат влијание на содржината кои треба да распределат за програмирање на hash функцијата (via DigestMethod). Крајната вредност на „hash“ е зачувана како „DigestValue“.
- *„SignatureValue“* е вистиската програмирана вредност на потписот. Поретко од дигиталното потпишување на содржината, потписот е програмира со „SignedInfo“ така што сите рефенци, алгоритми и крајни вредности се дигитално заеднички потпишани со што се обезбедува интегритетот на потпишаните податоци.
- *„KeyInfo“* овозможува примачот да го добие клучот за да го потврди потписот ако е потребно. Структурата на фунцијата е многу комплексна.
- *„Object“* елементот содржи нелогични „XML“ податоци кои може да се рефенцираат во рамките на „SignedInfo“. Тој, исто така, може да вклучи „Manifest“ елемент кој обезбедува разнолика листа на референци, каде што

интегритетот на листатата самостојно е проверуван и каде што интегритетот на објектот нема да влијае на потписот. Намената на листата е да вклучи листа на објекти кои би требало да се во корелација со „manifest“. Тој исто така дефинира елемент на „SignatureProperties“ во кој се снимени други карактеристики на потписот како време и датум кога потписот е создаден.

```
<Signature Id-"MySignature"
xmlns="http://www.w3.org/2000/0 9/xmldsig#">
<SignedInfo>
<CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-d4n-
20010315"/>
 <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-shal"/>
<Reference URI="http://www.company.ccm/file.doc">
<Transforms>
<Transform
 Algorithm="http://www.w3.org/TR/2001/REC-xml-cl4n-20
010315"/;
 </Transforms>
<DigestMethod
Algorithm="http://www.w3.org/2  0 0 0/0 9/xmldsig#shal"/>
<DigestValue>j90j2fnkfew3...</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>GFh8fw3greU...</SignatureValue>
 <KeyInfo>
 <KeyValue>
<DSAKeyValue>
<P>. . .</PXQ>. . .</QXG>. . .</GXY>. . .</Y>
</DSAKeyValue>
</KeyValue>
</KeyInfo>
 </Signature>
```

Слика 20. Пример на код за „XML Signature“ ([84])

Стандардот „XML signature“ дефинира три типа на дигитални потписи како *„enveloped“, „enveloping“,* и *„detached“*. „Enveloped signature“ се однесува на потпис на „XML“ податоци без разлика каде се наоѓа „Signature“ елементот во телото на „XML“. „Enveloping signature“ содржи „XML“ содржина која е потпишана онаму каде „Object“ елементот е употребен да содржи податок кој е потпишан. На крај „detached signature“ означува содржина која е надворешна за „XML signature“ дефинирана со „URI“ при што истата може да има надворешна дигитална содржина, но исто така може да вклучи елементи во рамките на „XML“ податоците како сродни елементи.

Како што беше претходно наведено, „XML signature“ дозволува секој тип на дигитална содржина да биде потишан и се употребува со стандардот „Web Services Security“.

„XML Encryption“ (Слика 21) Според дизајнот, „XML“ има едноставен текстуален формат без вградена безбедност. „XML encryption“ обезбедува доверливост на податоците преку механизам за шифрирање на „XML“ содржината каде што се користи симетричен клуч за шифрирање. Стандардните техники за размена на клучевите се

базирани на криптографијата за размена на јавните клучеви при што се обезбедува тајност за клучот што треба да се користи од повеќе корисници. Типично симетричниот клуч е вклучен во рамките на „XML“ пораката во криптирана форма, одредено е име за истиот, „URI“ или е добиен од размената на податоци за клучевите. За споредба, симетричниот клуч се употребува за да ги шифрира податоците наменски, бидејќи јавниот клуч е многу спор.

```
<EncryptedData Id? Type? MimeType? Encoding?>
<EncryptionMethod/>?
<ds:KeyInfo>
<EncryptedKey>?
<AgreementMethod>?
<ds:KeyName>?
<ds:RetrievalMethod>?
<ds:*>?
</ds:KeyInfo>?
<CipherData>
<CipherValue>?
 <CipherReference URI?>?
</CipherData>
<EncryptionProperties>?
</EncryptedData>

? = Zero or One Occurrence
+ = One or More Occurrences
* = Zero or More Occurrences
```

Слика 21. Синтакса на неформален „XML encryption“ ([84])

Како „XML signature“ така и „XML encryption“ е презентиран како „XML“. Струкурата на „XML encryption“ ги содржи следните елементи:

- *„EncryptedData“* е елемент кој идентификува дека тоа е шифриран податок;
- *„EncryptionMethod“* го дефинира алгоритмот за шифрирање кој е употребен за шифрирање на податоците како „Triple-DES“ (3DES). Ова е опционален елемент и ако не е презентиран тогаш мора да се знае кој алгоритам да се употреби за дешифрирање на податоците.
- *„ds:KeyInfo“* содржи информации за шифрираниот клуч кој бил употребен за шифрирање на пораката, при што вистинскиот клуч е вметнат во шифрирана форма или тоа се информации кои овозможуваат клучот да биде пронајден или изведен.
- *„EncryptedKey“* содржи шифрирана форма на клучот кој треба да се сподели. Како што беше претходно напоменато, овој клуч ќе биде шифриран со употреба на криптографија за јавни клучеви. Можно да има повеќе примачи на пораката за клучот, но за секој има шифриран елемент за клучот.
- *„AgreementMethod“* е алтернативен начин на споделување на клучот со употреба на метод како „Diffie-Hellman“. Со помош на методот се постигнува невметнување на клучот во „EncryptedKey“ елементот.
- *„ds:KeyName“* обезбедува дополнителен начин за споделување на клучевите според нивното име.
- *„ds:RetrievalMethod“* е начин за повторно враќање на шифрираната форма

на клучот од „URI“ референцата, без разлика дали се содржи во рамките на „XML“ или екстерно.

- *„ds:* refers“* се однесува за постоењето на други информации за клучеви како „X.509v3 keys“, „PGP keys“, и „SPKI“ клучеви кои може да бидат вметнати
- *„CipherData“* е елемент кој го содржи шифрираниот податок со „CypherValue“ како шифриран податок со „base64“ текст или со употреба на „CypherReference“ која ќе се однесува на местото за шифрираниот податок во „XML“ или некое друго место.
- *„EncryptionProperties“* содржат дополнителни карактериситки како време и датум на шифрирање.

```
<EncryptedData
xmlns='http://www.w3.org/2001/04/xmlenc#'
Type='http://www.w3.org/2001/04/xmlenc#Element'/>
<EncryptionMethod
Algorithm='http://www.w3.org/2001/04/xmlenc#tripledes-
cbc'/>
<ds:KeyInfo
xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
<ds:KeyName>John Doe</ds:KeyName>
</ds:KeyInfo>
<CipherData><CipherValue>F59E7F12</CipherValue></Cip
herData>
</EncryptedData>
```

Слика 22. Пример за „XML-encrypted message“ ([84])

Слика 22 претставува пример за „XML“ шифрирана порака. Шифрираните податоци се гледаат во „CipherValue“ елеметот

„XML signature“ и „XML encryption“ стандарди заедно ги формираат основите врз кои се потпираат „WS-S“ стандардите.

„SAML“ (Security Assertion Markup Language) ([92]) е стандардна околина базирана на „XML“ за комуникација со корисничкиот идентитет, корисничките карактериситки и привилегии помеѓу организациите или ентитетите во раздвоени сигурносни домени. „SAML“ се користи заедно со „XML signature“ и „XML encryption“ за да се овозможи интегритет, доверливост и автнтификација на „SAML assertion“.

„SAML“ дозволува ентитетот или организацијата да гарантира за идентитетот на корисникот преку „SAML assertion“. „SAML assertion“ може да биде презентиран како доказ за идентитетот на друг ентитет обезбедувајќи релации на доверба. Наведеното е многу важно за СОА бидејќи сервисите се лоцирани во различни компании и безбедносни домени. Концептот преставува основа за федеративен идентитет, кој ги штити организациите и овозможува менаџмент со автентификацијата и идентитот со други други организации.

Со „SAML“ се настојува да се решат неколку проблеми:

- „Web“ единствен „sign-on“ – каде корисникот може да пристапи на одредена

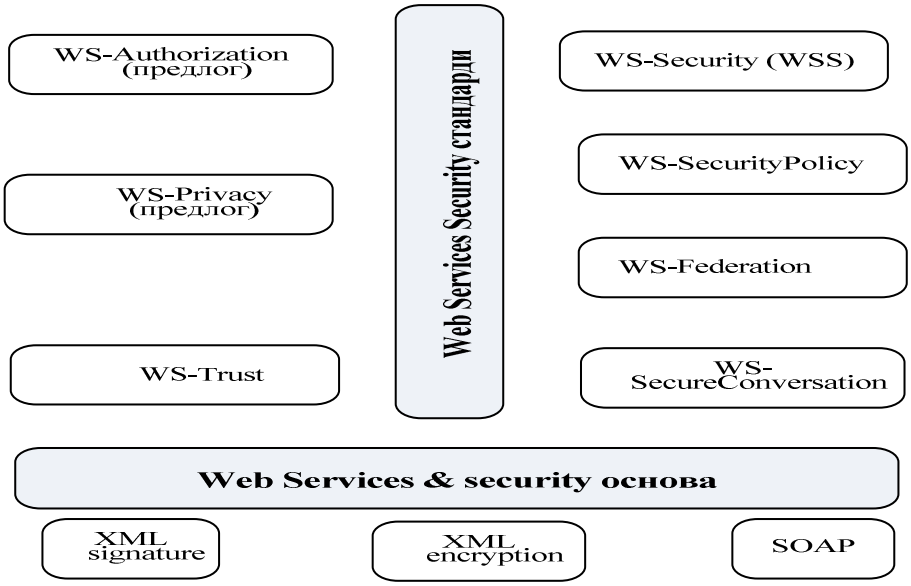
веб страна и потоа да пристапи на друга поврзана веб страна користејќи ги параметрите („SAML assertion“) на претходната.

- Доделен идентитет – параметрите добиени од почетната веб страна или сервис да може да се употребат за извршување на некоја услуга во името на друг корисник. Пример е веб страна на туристичка агенција, каде корисничкиот идентитет се користи од друг сервис со цел да се направи резервација за авион, хотели итн.
- Контролиран „sign-on“ – подразбира дека посредувачки сервис за безбедност ја контролира автентификацијата на корисникот. Параметрите добиени со посредувачкиот сервис за безедност потоа може да се користат за автентификација на различни веб страни;
- Автентификација базирана на атрибути – подразбира дека атрибутите или параметрите за корисникот се вметнати во „SAML assertion. Овие атрибути може да се користат за авторизациското одлучување. На пример "John Doe" има ниво на директор во секторот за човечки ресурси, при што врз основа на овие атрибути на него му се одобрува пристап до системот за човечки ресурси.

Во рамките на „SAML assertion“ можно да се вметнат информации за идентитетот на корисникот, како е-мајл адреса, „X.509“ име за субјектот , „Kerberos“ име или пак атрибути како идентификаскиот број на вработениот. За класифицирани намени и употреба „SAML 2.0“ воведува концепт на псевдоними (или идентификација по псевдоними) која може да биде искористена наместо други типови на идентификатори со цел да се сокријат персоналните информации за идентификација како е-мајл адресата. „SAML“ обезбедува два начини за потврдување на идентитетот на субјектот. Еден начин е „holder of key“, каде праќачот на пораката (субјектот) го „држи“ клучот кој бил употребен за дигитално потпишување на пораката. Другиот метод за потврдување е „sender vouches“, што подразбира дека дигиталниот потпис на пораката бил креиран од посреднички безбедносен сервис на кој може да му се верува.

Описот за „SAML“ е со намера да се објасни неговото искористување во СОА. Со зголемување на довербата помеѓу сервис провајдерите „SAML“ обезбедува слаба споеност (*engl.* loose coupling) и независност, но при тоа запазува идентитетот на корисникот. „SAML“ исто така се поврзува со „WS-S“ стандардите како безбедносен токен.

„*Web Services Security“ стандарди* ([93]) се опишани преку „Web Services Security“ протоколи (види Слика 23). Дијаграмот покажува дека „XML signature“, „XML encryption“ и „SOAP“ се основата за другите „Web Services Security“ стандарди.



Слика 23. WS-S стандарди

Од Слика 23 е јасно дека „WS-Security“ протоколот е комплексен. „WS-S“ ([89],[94]) се воспоставуваат на „SSL“ и на полисите за комплексноста на „firewall“ со цел да се обезбеди „point-to-point“ безбедност за „SOAP“ пораките. Со цел да се поедностави интеграцијата на безбедноста во „Web services“ и COA развиени се голем број на алатки.

5.4 Модел на сигурносно решение за ИСР

Согласно Слика 15 од ГЛАВА 4 е предложен модел на сигурносно решение за информацискиот систем за разузнавање. На сликата се презентирани два тека: контролен тек (плава линија) и податочен тек (црвена линија). „XML Signature“ стандардот е употребен во контролниот тек да изврши валидација на сигурносните полиси, додека валидација на сигурносните полиси во податочниот тек се извршува со „XML Encryption“ стандардот.

Сигурносното решение за информацискиот систем за разузнавање се базира на опишаните стандарди во секција 3. Со цел да се поедностави описот, во предложениот модел не е објаснето како се имплементирани полисите на дигиталните сертификати, бидејќи лесно може да се заклучи дека тие се наоѓаат во Центарот на ИСР.

На слика 9 се означени два значајни тека за ИСР, по следното:

- контролен тек;
- податочен тек.

Информациите кои поминуваат низ двата тека, исто така поминуваат низ три фази:

1. Фаза на евиденција – идентифукување на барателот на информациите и регистрирање на барањето, користијќи сигурносните механизми опишани во секција 3;
2. Фаза на верификација – идентификување на барателот на информациите и соодветноста на неговите сигурносни механизми, врз основа на безбедносните полиси кои се однесуваат за побараната информација;
3. Фаза на нотификација – врз основа на сигурносните механизми и полиси, барателот на информацијата е известен за користење на информациите од

сервисите или истиот е известен дека не е дозволено користење на сервисите, при тоа се праќа порака за причинита, согласно сигурносните полиси.

Побараната информација се пренесува од изворот на информации (сервисите) до барателот на информацијата, при тоа поминувајќи низ компонентите за медијација кои се користат за поврзување и форматирање на сигурносните системи во институциите. Медијациската компонента е значајна за ИСР, бидејќи преку неа се овозможува конекција со повеќе информациски системи кои се вметнати во хетерогена околина. Бараната информација е енкриптирана и има единствена сигурносна полиса. Иако Центарот на ИСР и регистарот на системот (*engl.*System Registry) не се инволвирани во првата фаза, тие играат значајна улога во втората и третатта фаза.

Контролниот тек извршува три функции:

1. Забележување на барателот на информацијата во однос на времето, датум, локацијата и типот на корисник на информацијата;
2. Валидација на сигурносните полиси според типот на корисникот, односно барателот на информацијата и валидацијата на сигурносните полиси кои се однесуваат на информацијата;
3. Забележување на секое барање кое не е пропратено со потребните информации во моментот на доставување на барање. Оваа функција потребно е да биде предмет на размислување за дизајнерите на информациски системи кои ќе ги дизајнираат идните сервиси.

Комплексно структурираниот предложен модел на сигурносно решение за иформацискиот систем за разузнавање базиран на СОА, не содржи само разнолики сигурносни механизми, туку се постигнува следното:

- Ефикасен пренос на податоци соодветно енкриптирани и форматирани на задоволително ниво;
- Забележување на секое барање, без разлика дали се наоѓа во базата на податоци или не, при тоа оценувајќи ја сигурносната полиса во однос на дозволен или недозволен пристап. На наведениот начин се може да се забележат можните нарушувања за сигурносната полиса;
- Флексибилни скалабилни механизми и механизми за проширување на употребата на сервисите кои се лоцирани во регистрите на ИСР.

ГЛАВА 6

МЕТРИКИ ЗА МОДЕЛ НА ИНФОРМАЦИСКИ СИСТЕМ ЗА РАЗУЗНАВАЊЕ БАЗИРАН НА СОА

Во ова поглавје е опишан модел на информациски систем за разузнавање базиран на сервисно ориентирана архитектура, при што тежиштето е насочено во креирање метриките кои се однесуваат на опишаниот модел на информациски систем за разузнавање.

Придонесот во поглавјето е презентиран преку развој на метрики кои ќе овозможат евалуирање на одредени принципи („unique categorization“, „discoverability“, „loose coupling“, „autonomy“) карактеристични за развој на сервисите во сервисно ориентираната архитектура. Во ист контекст ќе бидат воведени метрики за евалуирање на *достапноста* на разузнавачката информацијата до определен сервис, проценка на *веродостојноста* на информација, како и проценка на *чинењето* на информациската аквизиција.

Поглавјето е поделено во неколку секции. Во првата секција даден е преглед на истражувања во однос на развој на метрики за информациски системи. Секција 2 дава опис на сервисната структура на модел на информациски систем за разузнавање базиран на сервисно ориентирана архитектура. Секција 3 го разработува пристапот на сервисни договори (*engl.* service contract based approach) што ги дефинираат спецификациите на сервисот. Тие пак ги дефинираат функциите на учесниците во сервисот (како корисник и провајдер) и интерфејсите кои ги имплементираат со цел да ги исполнат задачите во сервисот. На крај, во Секција 4 се разработени метриките за сервисите и системот во целина.

6.1 Преглед на истражувања поврзани со поглавјето

Во ([102]), метриките за квалитетот на ресурсите (*engl.* resource quality) претставуваат димензија за проценка на квалитетот на софтверот (*engl.* software quality), при што истата метрика се однесува на проценување на сервисно ориентираната архитектура. Во трудот се разработени метрики за ресурсите (*engl.* resource metrics) за дистрибуираните системи кои ги поддржуваат сервисно-ориентираните концепти. Сличностите и разликите помеѓу решенијата за сервисно-ориентираниот пристап, веб базираниот пристап и софтверско-компонентискиот инженеринг (*engl.* component-based и web-based software engineering) се анализирани во контекст на инволвирани или искористени ресурси и нивното влијание на квалитетот.

Во ([97]) се нагласува дека сервисно ориентираната архитектура во денешницата претставува современо решение за развој на дистрибуирани апликации кои се користат како интеркомпаниски (*engl*. enterprise-wide) или за меѓукомпаниско бизнис работење (*engl*. cross-enterprise). Од аспект на софтверско инженерство, овие апликации изгледаат како софтверско-компонентски и објектно-ориентирани базирани системи и веб апликации, но разликите се доволно големи за да е едноставно невозможно да се

искористат постоечките метрики. Во трудот е направен обид да се анализираат овие разлики и да се формулираат метрики за продуктот (*engl.* product metrics) кои ги опфаќаат сите карактеристики на сервисно-ориентираниот софтвер во однос на проценката на комплексеноста, доверливоста и перформансите.

Во ([98]) важноста за мерењето на софтверот за време на фазата на развој е генерално прифатени во денешницата. Но, за несреќа во пракса општо прифатените алатки за мерење на софтверот наидуваат на многу мала прифатеност поради високите цени и нивната нефлексибилна структура. Од тие причини, во трудот е разработена структура за мерење на инфраструктурата во сервисно ориентираната архитектура.

„ISO/IEC 15939“ стандардот е селектиран за користење во истражувањето. Со употреба на метамоделот и онтологиите, кои се однесуваат за сервисите се овозможува нивна категоризација и класификација. Во трудот е презентирана онтологија базирана на веб сервиси подредена на објектно-ориентирани метрики како пример за компоненти на сервисно ориентирана инфраструктура. Прикажаните анализи за интеграционите аспекти го претставуваат начинот за подобрување на инфраструктурата со нова функционалност согласно „ISO/IEC 15939“ стандардот.

Во ([101]), во контекст на сервисно ориентираната архитектура, се идентифукувани атрибутите за квалитет (*engl.* quality attributes), како слаба поврзаност (*engl.*loose coupling) и автономност (*engl.*autonomy), кои што сервисите треба да ги исполнат. Со цел да се влијае во почетната фаза на креирањето на сервисите, земајќи ги во предвид атрибутите за квалитет, потребно е да се направи евалуација за време на почетната фаза на развој, односно за време на нивното дизајнирање. Моменталните истражувања се фокусираат на текстуалниот опис на посакуваните атрибутите за квалитет, при што формализираат метрики кои бараат повеќе информации отколку што има на располагање за време на дизајнирањето или се базираат на теоретски модели кои го оневозможуваат практичното искористување. Во трудот се разработени индикатори за квалитетот (*engl.* quality indicators), за единствена категоризација (*engl.*unique categorization), слаба поврзаност, откривност (*engl.*discoverability) и автономност. За секој индикатори за квалитетот, формализираните метрики се креирани со цел да овозможат мерење и користење во сервисните кандидати (*engl.* service candidates) и сервисниот дизајн во „Service oriented architecture Modeling Language“ (SoaML), како стандардизиран јазик за моделирање на сервисно-ориентираните архитектури. Со цел да се илустрираат метриките и да се верификува нивната валидност, евалуирани се сервисните кандидати и сервисниот дизајн на „Campus Guide System“ разиен од „Karlsruhe Institute of Technology“ (KIT).

6.2 Сервисна структура на информацискиот систем за разузнавање

Целта за имплементација на ИСР на стратегиско ниво, а тоа е најчесто државното, е централизирано собирање на разузнавачките податоци и нивно публикување во стандарден облик. Заради разноликоста на секторите и агенциите, врз информациските системи може да се применат различни концепти. Најчесто се применуваат хиерахискиот и дистрибуираниот концепт ([99]).

Хиерархиската структура подразбира собирање на податоци од пониските организациони нивоа. На овој начин, податоците сукцесивно се собираат и стигнуваат во највисокото ниво на ИСР. Предноста во овој пристап е дека секој ИСР е одговорен за мал број на извори на пониските нивоа. Но, доколку системот се организира на овој начин,

потребно е да се имплементира на поголем број подсистеми, при што ќе се појават потешкотии за стандардизирање на податоците на различни нивоа ([99]).

Од друга страна ИСР може да се дизајнира и спрема дистрибуираниот модел на податоци. Ваквиот начин на пристап подразбира и постоење на единечен ИСР кој собира податоци од различни системи, без разлика на нивната различност во поглед организационото ниво на кое се имплментирани. На тој начин, многу лесно се дефинираат стандардите, а податоците се централизирани. Недостаток на овие системи е тоа што само еден ИСР е одговорен за податоците од големиот број на извори. Таквата задача во пракса може да биде многу сложена за само еден ИСР ([99]).

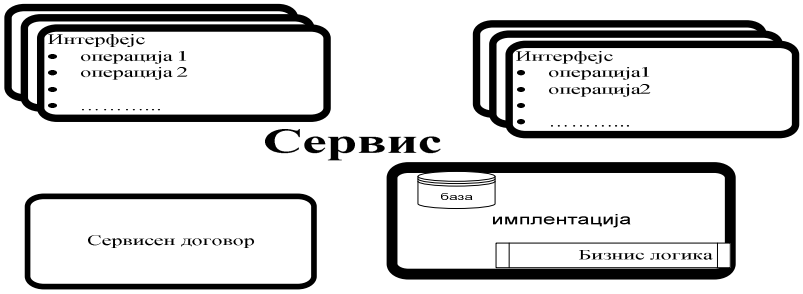
Во пракса, најчесто се сретнуваат системи кои по својата природа се хибридни, односно кои ги комбинираат овие два пристапа, што не значи дека не треба да се настојува во имплементација само на системи со дистрибуирана структура ([99]).

СОА претставува современ пристап за градење на дистрибуирани апликации кои ги надминуваат „границите“ на компаниите. „Блоковите за градење“ на овие апликации се сервисите независни софтверски ентитети, чии функционалности и метаподатоци дозволуваат едноставен пристап преку мрежа. Всушност, многу технологии може да се употребат за имплементирање на сервисите, скоро секој тип на дистрибуираните компоненти, на пример веб сервиси, „CORBA“, „DCOM“, „EJB“ и други, кои може да се користат за изградба на СОА основата ([97]).

СОА концептите и технологиите се широки прифатени и адаптирани во индустријата. Тоа предизвикува потреба од развој на методи за проценка на СОА инфраструктурата. Затоа во овој труд е предложено множевство од метрики кои ќе се употребат за проценка на некои квалитативни карактеристики на сервисно-ориентираните системи. Потребно е да се нагласи дека сервисно ориентираната архитектура е пристап, а не продукт. Дистрибуираните софтверски сиситеми изградени врз основа на СОА, односно имплементација на СОА принципите, „SOA as a thing” ќе се означува во трудот „service oriented system” (или едноставно “system”) ([97]).

Сервисно-ориентираниот систем се состои од множество на провајдерски точки. Секоја од точките обезбедува немобилни сервиси, а секој сервис има една или повеќе операции (бизнис функции). Клиентите како „end-user GUI“ апликациите, „service choreography“ или „orchestration engines“, или други сервиси, комуницираат со сервисите (ги вовлекуваат нивните операции) во смисла на размена на пораки. Асинхронизираниотот и синхронизираниот начин на комуникација е возможен, но првиот има тенденција да биде доминантен ([97]).

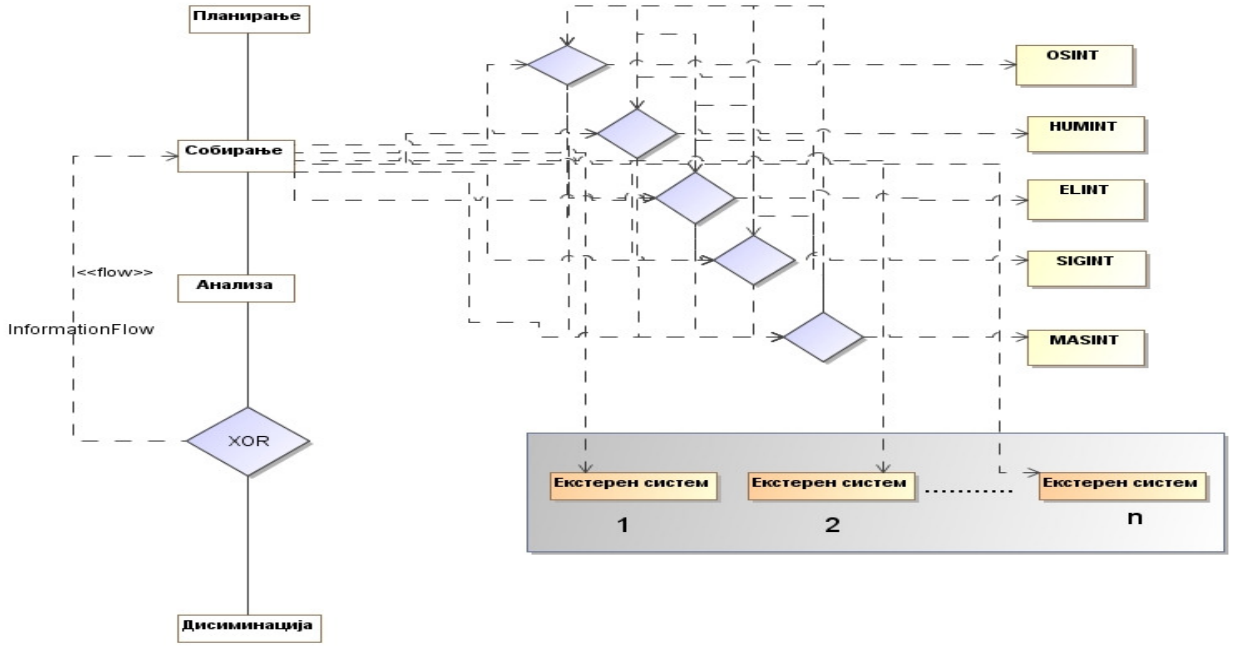
Сервисот претставува основен елемент во СОА – енкапсулација на бизнис концепт на ниско ниво. Се карактеризира со имплементација која е реализирана со бизнис логика и податоци, *сервисен договор* (*engl. Service Contract*) кој ја дефинира функционалноста, условите за користење и ограничувања за клиентите и *интерфејс* со кој физички се претставува функционалноста на сервисот (Слика 24).



Слика 24. Структура на сервисот во сервисно ориентирана архитектура

Сервисите можат да бидат едноставни (*engl.*atomic) или комплексни (*engl.*compound), при што претставуваат структурирана компонента од повеќе сервиси. Во случај на управувањето со бизнис процесите (*engl.* Business process management (BPM)), комплексните сервиси треба да се користат во оркестрирани бизнис процеси (во зависност од големината може да се нарекуваат и апликации) ([97]).

На сликата (Слика 25) е претставен бизнис процес за собирање на разузнавачки информации. Бизнис процесот е базиран на разузнавачкиот циклус. Насоките и планирањето кои информации се потребни за креирање на „мозаикот“ од информации се даваат од авторитетите.



Слика 25. Бизнис процес за собирање на информации

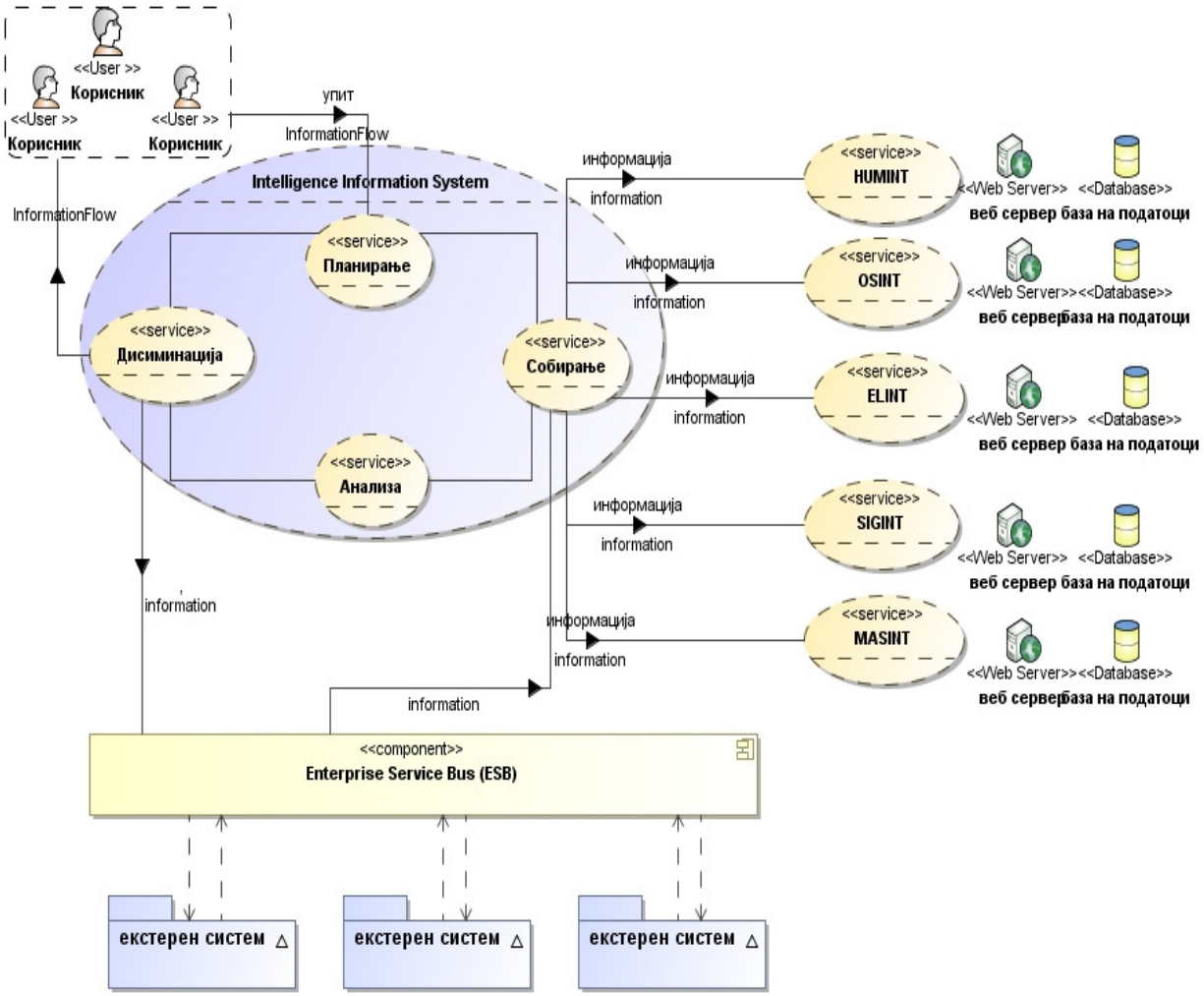
Откако ќе се добиени насоките од авторитетите, се пристапува кон собирање на информации. Собирањето на информации се одвива низ повеќе процеси. Како крајни точки се појавуваат изворите на инфомации или разузнавачките дисциплини („Imagery Intelligence“ (IMINT), „Signals Intelligence“ (SIGINT), „Measurement and Signature

Intelligence“ (MASINT), „Electronic Intelligence“ (ELINT), „Open-source Intelligence“ (OSINT), „Human Intelligence“ (HUMINT)) на кои се основа разузнавањето. Бројот на процесите кои треба да се реализираат не треба да влијаат на собирањето на потребните информации. Надворешните системи играат значајна улога во собирањето на разузнавачки информации и истите се користат како надворешни точки за кои е потребно да се дисиминираат информации.

Информациите кои се добиени со собирање се анализираат. Процесирањето на добиените информации е со цел да се креира збирна информација. Доколку се воочи потреба од дополнително собирање на информации, процесот повторно отпочнува со собирање на потребните информации.

Завршен чекор во бизнис процесот е дисиминацијата на информациите. Информациите може да се дисиминараат согласно претходно утврдени процедури, се со цел избегнување на грешки во дисиминацијата.

Исто така на Слика 26 е претставен модел на информациски систем за разузнавање базиран на СОА, кој треба да ги поддржи бизнис процесите кои се одвиваат во разузнавањето претставени на Слика 25.



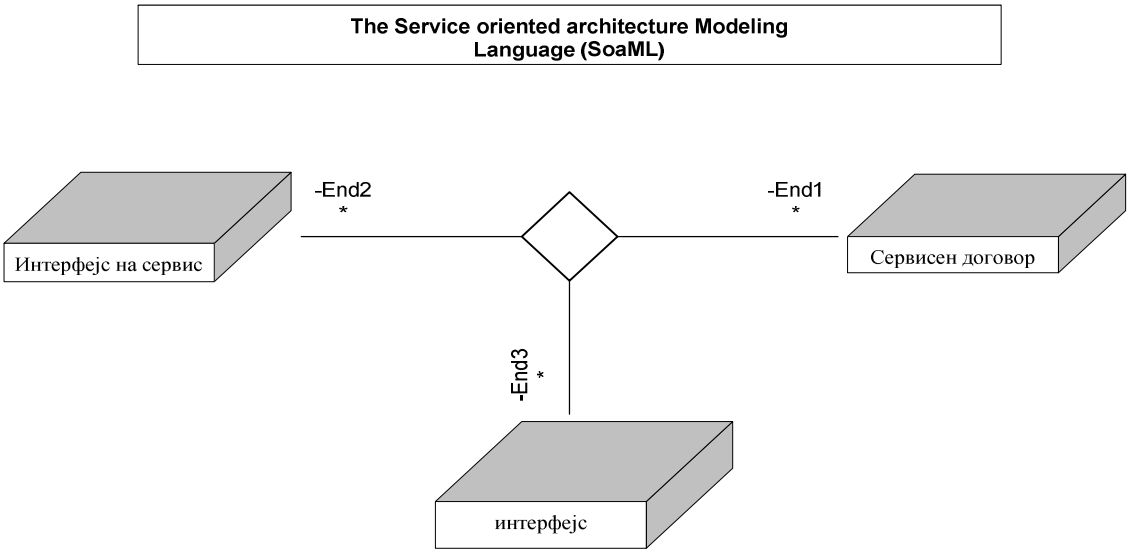
Слика 26. UML модел на информациски систем за разузнавање базиран ана СОА

6.3 Сервисни договори

„SoaML“ (*engl.* Service oriented architecture Modeling Language) спецификацијата (OMG, 2009) дефинира „UML“ профил и метамодел за дизајнирање на сервиси во рамките на сервисно ориентираната архитектура. Целите на „SoaML“ е да ги подржи активностите при моделирање и дизајнирање на сервисите и да ги вметне во „model-driven development approach“ (MDA), подржувајќи ја COA во бизнис и „IT“ перспективите ([100]).

„SoaML“ спецификацијата дефинира три различни решенија за специфицирање на сервисите:

- Решение на едноставен интерфејс (*engl.*simple interface) користи „UML“ интефејс за еднонасочна сервисни интеракција (*engl.* one-way service interaction) [100];
- Решение на сервисни договори (*engl.*service contract) ја проширува „UML“ колаборацијата за специфицирање на бинарната (*engl.*binary) или повеќенасочната (*engl.* n-ary) сервисна интеракција ([100]);
- Решение на сервисни интерфејси (*engl.* service interface) ја проширува „UML“ класата за специфицирање на бинарната или повеќенасочната сервисна интеракција ([100]).



Слика 27. „SoaML“ (*engl.*Service oriented architecture Modeling Language)

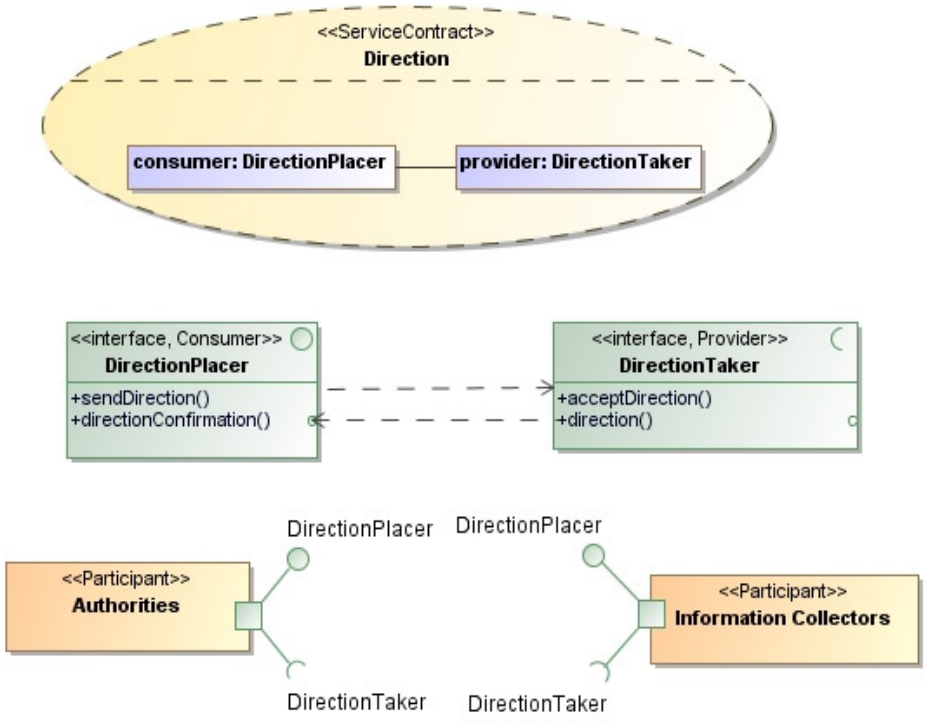
Различните решенија од „SoaML“ пропишуваат употреба на различни делови од „UML“, при што разбирањето како тие се поврзани не е очигледно од самото читање на спецификацијата. Поради наведената причина се појавуваат проблеми во дизајнирањето на информациските системи во софтверското инжинерство ([100]).

Пристапот на сервисни договори ги дефинира спецификациите на сервисот кои ги дефинираат функциите на учесниците во сервисот (како корисник и провајдер) и интерфејсите што ги имплементираат со цел да ги исполнат функциите на сервисот. Овие интерфејси се видови на портови за одреден учесник кои бараат од учесникот да ја изврши функција во одредениот сервисен договор ([100]).

Пристапот на сервисни договори овозможува подобра презентација на сервисите со користење на „UML“ модел на соработка за структурниот дел од сервисна интеракција. Пристапот може да може да се употреби за специфицирање на сервиси во кој има договорени обврски, како на пример договор помеѓу две или повеќе страни. Тоа се применува во случаи во кои постои интеракциска шема која вклучува размена на пораки кои специфицираат (едноставен) интерфејс на двете страни ([100]).

Од информацискиот систем за разузнавање ќе употребиме одредени сервиси со цел да ја демонстрираме употребата на пристапот базиран на сервисни договори со цел да го дефинираме бинарниот или двонасочниот сервисен договор (*engl.* binary service contract), комбинираниот сервисен договор (*engl.* multi-party service contract) комплексниот сервисен договор (*engl.* compound service contract). Прво да претпоставиме дека „Direction service contract“ може да се моделира како два независни сервисни договори, при што еден ќе ја специфицира интеракцијата за давање на насоки за собирање на информации, а другиот ќеја специфицира интеракцијата за прифаќање на насоките за собирање на информации. Слика 28 ја прикажува спецификацијата на „Direction service contract“, со две функции на корисник и провајдер и нивните интерфејси „DirectionPlacer“ и „DirectionTaker“ ([100]).

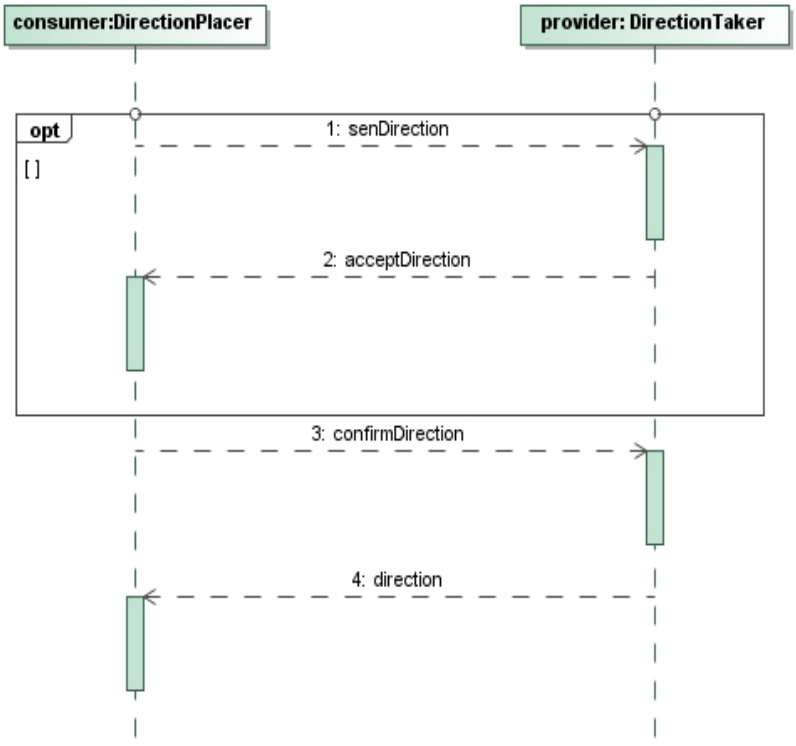
Серивисниот договор покажува дека постојат зависности помеѓу двата интефејса и тие мора да бидат моделирани со „UML dependicies“. Учесниците со интеракцијата во сервисниот договор ја извршуваат својата функција со користење на соодветните интефејси и опишувајќи ги истите преку портови. Од улогата на поврзување во сервисната архитектура, ние може да заклучиме дека „Authorities“ има порт внесен преку „DirectionPlacer“ интефејсот и „Information Collectors“ има сервисен порт внесен преку „DirectionTaker интерфејсот“.



Слика 28. Спецификација на „Direction“ сервисот

Во наведениот пример сервисниот договор претставува елемент од два интерфејса, кои претставуваат дел од една сервисна спецификација со два различни едноставни интерфејси. Како дополнение на структурната спецификација потребно е да се специфицира компонента за интеракција на сервисот со „SOAP“ протоколот (*engl.* behavior) на сервисниот договор, односно кореографијата на сервисите.

На Слика 29 подолу се прикажува спецификацијата за кореографија на сервисите (*engl.* service choreography) со употреба на „UML“ интеракција. Може да се види дека е специфицирана конверзација, односно размена на пораки, помеѓу двајца учесници, при што се бара имплементирање на два интефејси од двете страни.

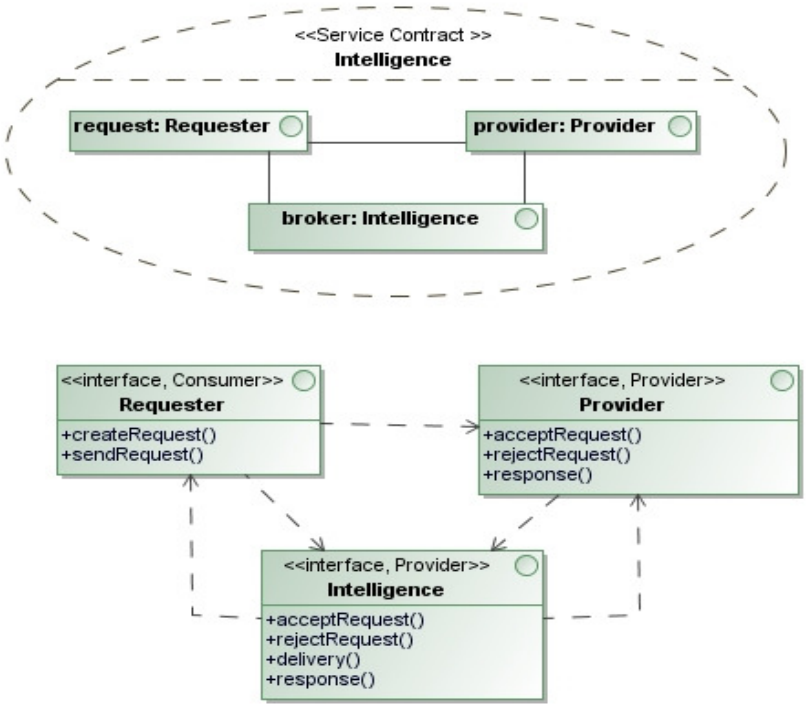


Слика 29. Спецификација на кореорафијата на „Direction“ сервисот

Решението базирано на сервисен договор е соодветно кога имаме специфицирање на интеракции помеѓу две или повеќе улоги (*engl.* roles) кои се воведуваат за воспоставување на договор (*engl.*agreement), како на пример за размена на пораки. Сервисниот договор исто така се употребува како реупотреблив спецификациски елемент кој може да биде реупотребен во времето на дизајн за да ги поврзе различните учесници. Понатаму, решението исто така подржува моделирање на комбинирани (*engl.* multiparty) сервисни договори вклучувајќи најмалку три или повеќе учесници, потоа за комплексни сервисни договори (*engl.* compound service contracts), каде постоечкиот сервисен договор може да се употреби за дефинирање на повеќе грануларни сервисни договори (*engl.* granular service contracts.)

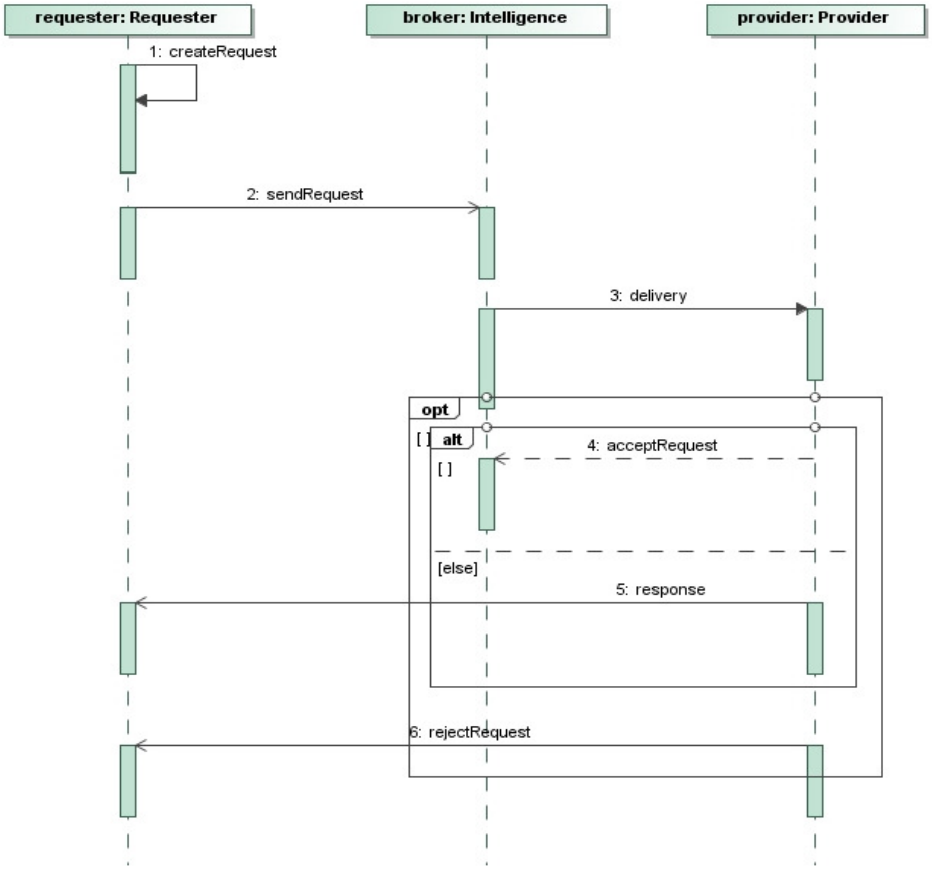
Прво ќе го погледнеме комбинираниот сервисен договор. Во нашиот пример е употребен „Intelligence service contract“, каде интеракцијата помеѓу барателот на информацијата и провајдерот е посредувана преку „Intelligence broker“. Слика 30 ја

прикажува спецификацијата на „Intelligence service contract“, со три улоги: барател на информација, провајдер и брокер и нивните одделни типови на интерфејси за корисник (*engl.* consumer) и провајдер наречени како „Requester“, „Provider“ и „Intelligence“. Зависностите помеѓу интефејсите се експлицитно моделирани со употреба на „UML dependencies“ каде учесниците имаат портови соодветни на функцијата за поврзување во сервисната архитектура.



Слика 30. Спецификација на сервисниот договор „Intelligence“

Слика 31 ја покажува спецификацијата на кореографија на сервисот со употреба на „UML“ интеракција. Треба да се забележи дека ова е комбиниран (*engl.* multiparty) сервисен договор, бидејќи барателот (*engl.* requester) има интеракција со провајдерот (*engl.* provider) на информации директно со пренесување (*engl.* delivery) на пораките. Со исклучок на пренесувањето на пораките, сите други интеракции се одвиваат преку посредник „broker: Intelligence“. Сервисната интеракција започнува со барање за информација спрема брокерот. По одредено време пренесувањето е напревено без разлика дали е прифатено или сторнирано. Тоа се праќа до брокерот кој го препраќа до провајдерот, а тој може да ја утврди валидацијата, сè со цел доенсе одлука за прифаќање или отфрлање на барањето.



Слика 31. Спецификација на кореографијата на „Intelligence“ сервисот

6.4 Метрики

За да може да се изврши правилно евалуирање на сервисите потребно е да постојат конкретни начини на мерење (метрики) ([101],[104]), како и вредност која укажува дали добиениот резултат е голем, мал или има некоја средна вредност.

Клучен фактор во работа со метриките е знаењето за правилно интерпретирање на добиената вредност. Од таа причина потребно е да се воведат гранични вредности. Граничните вредности се користат за споредување на добиената вредност со референтна вредност. Граничните вредности се одредуваат статистички или според прифатените семантички конвенции.

Атрибутите за дизајнот може да се употребат во креирање на карактеристиките на сервисот, користејќи ја „SoaML“ спецификацијата. Табела 1 претставува збир на идентификувани атрибути за дизајн. Врз основа на табела, ќе воведеме унифицирани метрики, кои се однесуваат на одредени атрибути за дизајн. Исто така од табелата, лесно се воочува дека некои атрибути за дизјан, не може да се представат со метрики.

Табела 1. Збирно идентификувани атрибути за дизајн ([101], [104]).

Карактеристики на дизајнот на сервисот	**Очекувани (*engl.* preferred) карактеристики во SoaML**
Автономност	
Капацитет за намалување на ризикот на грешки при дуплирање на информациите	Не постои ограничување за „Capability“ елементите на интерфејсот на сервисот кој ги ограничува капапцитетите на другите сервисни интефејси.
Зависни сервиси	Не постои точка на упит за учесниците.
Дизајн на интерфејсот на сервисот	
Содржина на сервисниот интерфејс	Сите информации (капацитет, протокол за интеракција, технички интерфејс) се содржат во соодветниот сервисен интерфејс.
Презентирање на сервисниот интерфејс (*engl.* formalization)	Постои елементот за сервисниот интерфејс.
Доверливост на податочниот модел	Операциите во технички интерфејс користат податочни типови од општи податочни модели.
Усогласени правила (*engl.* Convention Compliance)	сервисниот интерфејс, неговите операции и параметри во рамките на техничкиот интерфејс ги следат правилата за именување.
Комбинираност (*engl.*Coupling)	
Паралелна или мултипроцесорка работа на сервисниот интерфејс (*engl.* asynhronity)	Бараниот технички интерфејс постои и протоколот за интеракција ги опишува посакуваните асинхрони интеракции.
Податочни типови на сервисниот интерфејс	Технички интерфејс користи само едноставни податочни типови наместо комплексни податочни типови.
Генерализација на сервисниот интефејс (*engl.* abstraction)	Техничкиот интерфејс содржи операции и параметри кои ги кријат имплементациските детали.
Процес на трансакции (*engl.* Transaction Handling)	Доколку учесникот достави упит користејќи соодветна сервисна логика, во логиката треба да се содржат функции или пак преку техничкиот интерфејс се користат операции за функционирање.
Параметар метода	Операциите во рамките на техничкиот интерфејс користат параметерска метода на пораки за наместо метода на „Remote Procedure Call“ (RPC).
Апстракност (*engl.*Abstraction)	
Генерализација на сервисниот интефејс	Исто како Генерализација на сервисниот интефејс во Комбинираност.
Презентирање на сервисниот интерфејс	Исто како Презентирање на сервисниот интерфејс Дизајн на интерфејсот на сервисот.
Повторна искористливост (*engl.*Reusability)	
Агностичност на сервисните компоненти (*engl.* Agnosticity)	Логиката на учесникот може повторно да се употреби во повеќе процеси.
мултифункционален сервисен интефејс (*engl.* Genericity)	Периметарот на операциите во рамките на техничкиот интерфејс треба да е соодветен за широка употреба т.е повеќефункционален
Истовремено извршување на различни сервисни операции (engl. Concurrency)	Сервисната логика на учесникот треба да овозможи истовремено извршување на сервисите.
Способност за самосодржење (*engl.*Self-Containedness)	
Капацитет за намалување на ризикот на грешки при дуплирање на информациите	Исто како Капацитет за намалување на ризикот на грешки при дуплирање на информациите во Автономност.
Зависни сервиси	Исто како Зависни сервиси во Автономност.
Редослед на операциите	Не постои редослед на извршување на операциите помеѓу операциите во рамките на протоколот за интеракција и сервисниот интерфејс.
„Statelessness“	
Менаџмент со состојбата на сервисните компоненти	Логиката на учесникот не вклучува активности за зачувување на состојбата на одреден учесник.
Операциски параметри (*engl.*Operation Parameters)	Операциите во рамките на техничкиот интерфејс содржат параметарски типови на комплетни објекти наместо „ID“ за објекти.
Откривност (*engl.* Discoverability)	
Усогласени правила	Исто како Усогласени правила од Дизајн на интерфејсот на сервисот
Функционален сервисен интерфејс (*engl.* Functional Service Interface)	Техничкиот интерфејс содржи операции и параметри со разновидни функции. Интерфејсите и сервисите се соодветно именувани.
Способност за поврзување (*engl.*Composability)	
Разновидна грануларност (*engl.*Multiple Granularity	Постојат операции во рамките на техничкиот интефејс кои дозволуваат слична функционалност со различни елементи (*engl* granularity).
Постојаност (*engl.* Idempotency)	
Менаџирање со различни операциски упити (*engl.*Multiple Operation Call Handling)	Логиката на учесникот содржи активности за да се изменаџираат различни операциски упити истовремено.
Класификација (*engl.*Classification)	
Ентитети/Класификација на задачи	Сите капацитети во рамките на елементот „Capability“ се соодветни за менаџирање со податоците на бизнис ентитетите(*engl.* entity service) или содржат бизнис логика која се користи од бизнис ентитетите (*engl.*task service).
Дефинирање на сервисниот интефејс (*engl.* Service Interface Well-Definition)	
Содржина на сервисниот интерфејс	Исто како во Содржина на сервисниот интерфејс во Дизајн на интерфејсот на сервисот

6.4.1 Метрики за евалуација на сервиси

А. Единствената карактеризација (*engl. unique categorization*) се анализира преку четири сервисни индикатори: бизнис – ориентирана или техничка функционалност BT(s), агностичка или неагностичка функционалност AN(s), податочна супериорност DS(s) и употреба на заеднички бизнис ентитети CB(s) ([101]). Земајќи ги предвид посакуваните вредности на овие индикатори, докторската дисертација предлага користење на обединувачка метрика **K(s)** на единствената карактеризација на сервисите (или во рамки на сервис дизајнот, на сервис-кандидатите), за секој од следните случаи:

А.1. Бизнис ориентирана, агностичка функционалност:

$$K(s) = \frac{BT(s) + AN(s) + DS(s) + CB(s)}{4} \tag{6.1}$$

А.2. Функционално ориентирана, агностичка функционалност:

$$K(s) = \frac{1 - BT(s) + AN(s) + DS(s) + CB(s)}{4} \tag{6.2}$$

А.3. Бизнис ориентирана, неагностичка функционалност:

$$K(s) = \frac{1 + BT(s) - AN(s) + DS(s) + CB(s)}{4} \tag{6.3}$$

А.4. Функционално ориентирана, неагностичка функционалност:

$$K(s) = \frac{2 - BT(s) - AN(s) + DS(s) + CB(s)}{4} \tag{6.4}$$

Во секој од наведените случаи, вредноста на K(s) е во интервалот [0,1]. Посакуваната вредност во однос на единствената карактеризација на сервисите е 1.

В. Откривност (*engl. discoverability*), покрај тоа што е поврзана со единствената карактеризација, е опишана и со неколку други индикатори: функционалното именување FN(sc), усогласеноста со функционалното именување CFN(sc) и информацискатa содржина IC(sc). Овие индикатори се релевантни во процесот на сервисниот дизајн, па поради тоа ќе сметаме дека се однесуваат на сервисните кандидати. Се цел да формираме единствена метрика за откривноста **D(sc)**, дефинираме средна вредност за FN(sc) и CFN(sc), која ќе ги вклучи соодветните вредности за улогите (R), операциите (O), параметрите (P), податочните типови (T) и интерфејсите (I). Имаме:

$$\begin{aligned} FN(sc) &= \frac{1}{5}\left[FN_R(sc) + FN_O(sc) + FN_P(sc) + FN_T(sc) + FN_I(sc)\right] \\ CFN(sc) &= \frac{1}{5}\left[CFN_R(sc) + CFN_O(sc) + CFN_P(sc) + CFN_T(sc) + CFN_I(sc)\right] \end{aligned} \tag{6.5}$$

Метриката на откривност ја дефинираме на следниот начин:

$$D(sc) = \frac{FN(sc) + CFN(sc) + IC(sc)}{3} \tag{6.6}$$

Вредноста која притоа се добива е во интервалот [0,1]. Вредност еднаква на 1 укажува на максимална откривност, додека 0 означува нејзино непостоење.

C. Слабата споеност (*engl. loose coupling*) на сервисите ја зголемува нивната флексибилност, прилагодливост, отпорноста кон грешки и недостатоци како и одржливоста на архитектурата. Индикатори кои се релевантни во овој смисол се: асинхроноста на долгорочните операции AS(s), комплексноста на заедничките податочни типови CCT(s), апстракција на знаењето поврзано со имплементацијата на операциите и параметрите AN(s) и (не)компензација на операциите NC(s). Користејќи ги овие индикатори, формираме метрика на слаба споеност **LC(s)** на следниот начин:

$$\mathrm{LC}(s) = \frac{\mathrm{AS}(s) + \mathrm{CCT}(s) + \mathrm{AN}(s) + \mathrm{NC}(s)}{4} \tag{6.7}$$

(Забелешка: Овде, $\mathrm{AN}(s) = \frac{1}{2}(\mathrm{AN_O}(s) + \mathrm{AN_P}(s))$ е средна вредност на метриката на апстракција од одделно пресметаните метрики за операции и параметри.)
Слабата поврзаност е максимална доколку вредноста на дефинираната метрика е 1.

D. Автономноста (*engl.* autonomy) на сервисите ја опишуваат индикаторите на директна сервисна зависност SD(s) и на функционално преклопување FO(s), при што таа е обратнопропорционална на нивната вредност. Дефинираме обединувачка метрика $\mathbf{AU}(s)$ за автономност на следниот начин:

$$\mathrm{AU}(s) = \frac{\mathrm{SD}(s) + \mathrm{FO}(s)}{\mathrm{SD}(s) \cdot \mathrm{FO}(s)} \tag{6.8}$$

Вредноста на вака дефинираната автономност е во интервалот $[1, \infty]$. Притоа, $\mathrm{AU}(s) = 1$ означува најмала автономност, а зголемување на вредноста на оваа метрика укажува на зголемување на автономноста сервисот. Нагласуваме дека не постои горна граница за $\mathrm{AU}(s)$.

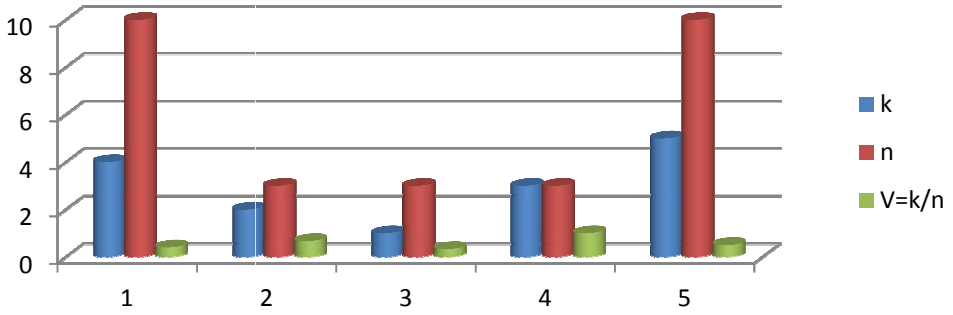
6.4.2 Метрики за евалуација на сервисите во информацискиот систем за разузнавање

Веродостојноста „V“ на информација добиена со посредство на даден сервис, се дефинира како веројатност за точност на таа информација. Оваа веројатност се утврдува емпириски според:

$$V = \frac{k}{n} \tag{6.9}$$

Табела 2. Веродостојноста „V“ на информација добиена со посредство на сервис

k	n	V=k/n
4	10	0.40
2	3	0.67
1	3	0.33
3	3	1.00
5	10	0.50



Слика 32. Графички приказ на веродостојноста „V“ на информација добиена со посредство на сервис

каде n е вкупниот број на информации добиени од сервисот во определен период на набљудување, а k е бројот на точните информации. Јасно, $V \in [0,1]$.

Разгледуваме систем за обезбедување на информации кој се состои од m сервиси, чие функционирање не е системски поврзано. Врз веродостојноста на ваквата информација ќе влијаат резултатите кои се обезбедени од секој поединечен активиран сервис. Притоа, *максималната веродостојност* на информацијата ќе биде:

$$V_{max} = \max_{\substack{\chi(i)=1 \\ i=1,m}} \left\{ \chi_A(i) \cdot \frac{k_i}{n_i} \right\} \tag{6.10}$$

каде $\chi(i)$ е функција на налогодавачот за прибирање информација,

$$\chi(i) = \begin{cases} 1 & \text{ако сервисот е активиран} \\ 0 & \text{во спротивно} \end{cases}$$

а χ_A е функција на бинарната карактеризација на информацијата која утврдува дали конкретната информација е добиена од сервисот i:

$$\chi_A(i) = \begin{cases} 1 & \text{ако информацијата е добиена од i} \\ 0 & \text{во спротивно} \end{cases}$$

За да може веродостојноста на добиените податоци да се анализира, потребно е вкупната информација да биде разбиена на *елементарни информации*. Како и погоре, појавувањето на ваквата информација во секој од сервисните известувања има бинарна карактеризација: 0 или 1. Тогаш, за секоја елементарна информација може да се определи очекувана точност или *средна веродостојност*,

$$V_E = \frac{\sum_{i=1}^{m} \chi(i) \chi_A(i) \cdot p_i}{\sum_{i=1}^{m} \chi(i)} \tag{6.11}$$

Може да забележиме дека добиените вредности во (10) и (11) зависат од множеството на активирани сервиси. Тоа значи дека одлуките за активирање на одделни сервиси директно ќе влијаат врз веродостојноста на добиената информација. За да се зголеми вредноста на очекуваната информациска точност, потребно е да се утврдат критериуми врз основа на кои ќе се донесуваат ваквите одлуки.

Еден од тие критериуми е секако, *достапноста* на информацијата до определен сервис. Вредноста d која ја изразува достапноста е проценка која се утврдува врз основа на претходни согледувања и познати факти, а се опишува преку број од интервалот $[0,1]$. Притоа, $d = 0$ означува дека информацијата е целосно недостапна, додека $d = 1$ дека таа е целосно достапна за сервисот. Со овие податоци можеме да ја изразиме „apriori" веројатноста за добивање на точна информација од сервисот i, како

$$(AV)_i = d_i \cdot p_i = \frac{d_i \cdot k_i}{n_i} \tag{6.12}$$

Максималната веројатност за добивање на точна информација од i ќе биде

$$(AV)_{i\_max} = \max_{\substack{\chi(i)=1 \\ i=1,m}} \left\{ \frac{d_i k_i}{n_i} \right\} \tag{6.13}$$

додека очекувањето за добивање на точна информација од активираните сервиси е

$$V_E = \frac{\sum_{i=1}^{m} \chi(i)\, d_i\, p_i}{\sum_{i=1}^{m} \chi(i)} \tag{6.14}$$

Оттука, доколку сакаме да обезбедиме максимално достапна и точна информација, притоа активирајќи s сервиси од достапните m, потребно е да го решиме следниот оптимизациски проблем:

$$\max_{\substack{S \in 2^m \\ |S|=s}} \left\{ \frac{1}{s} \cdot \sum_{i \in S} \frac{d_i k_i}{n_i} \right\} \tag{6.15}$$

каде 2^m го означува број на елементи во партитивното множество на $\{1,2,\ldots,m\}$.

Ќе забележиме дека споредувањето на резултатите од (6.10) и (6.13), односно на (6.11) и (6.14), може да укаже на исправноста на донесената одлука.

Друг елемент кој може да се земе предвид во планирачката фаза е чинењето на информациската аквизиција. Неговата процена може да ги опфати потребните ресурси, но и можниот ризик кој се презема во процесот. Оваа процена ја изразуваме номинално преку бројот u_i за сервисот i – притоа ќе ги земеме нормализираните вредности на u_i. Формирајќи *коефициент на аквизиција* $k_i = d_i / u_i$, во одлуката за активирањето на сервисите може да го вклучиме следниот програм:

$$\max_{\substack{S \in 2^m \\ |S|=s}} \left\{ \frac{1}{s} \cdot \sum_{i \in S} \frac{d_i k_i}{n_i u_i} \right\} \tag{6.16}$$

Неговото решение ќе ни ја даде онаа група од s сервиси, кои овозможуваат оптимална комбинација на достапност и исплатливост, во однос на веродостојноста на дадена елементарна информација.

Табела 3. Приказ на веродостојноста за добиена елементарна информација

сервис	n_i	k_i	V_i (Vmax)	$\chi(i)$	$\chi_A(i)$	V_E	d_i	$(AV)_i$	$(AV)_E$
1	2	3	4=3/2	5	6	7=∑4/1	8	9=8*3/2	10=∑9/1
1	10	8	0.80	1	1		0.7	0.56	
2	9	5	0.56	1	0		0.85	0.47	
3	7	6	0.86	0	1		0.5	0.43	
4	5	2	0.40	1	1		0.3	0.12	
5	8	5	0.63	0	1	**0.59**	0.95	0.59	**0.41**
6	2	1	0.50	0	0		0.9	0.45	
7	6	4	0.67	1	0		0.95	0.63	
8	10	1	0.10	1	1		0.7	0.07	
9	3	2	0.67	0	1		0.4	0.27	
10	4	3	0.75	1	0		0.7	0.53	

n_i – број на добиени информации од сервисот i
k_i – број на точни информации добиени од сервисот i
V_i – веродостојност на сервисот i
$\chi(i)$ **–** индикатор на активирање на сервис i (1- активен, 0- неактивен)
$\chi_A(i)$ – индикатор на добиена информација од сервисот i (1 - да, 0 - не)
V_E – средна веродостојност на информацијата
d_i – достапност на информацијата до сервисот i
$(AV)_i$ – веројатност за добивање на точна информација од сервисот i
$(AV)_E$ – очекување за добивање на точна информација од активираните сервиси

Теоретски, метриките воведени во информацискиот систем за разузнавање, укажуваат дека процесот на планирање, кои информации ќе се собираат и кој сервис ќе биде употребен за да се добие точна информација и процесот на анализа од друга страна кога добиените инфомации од сервисите се анализираат, укажуваат дека има одредени разлики.

Табелата 3 може да разгледува од два аспект и тоа од аспект на анализа на собраните информации и од аспект на планирање на собирањето на информациите кои од сервисите ќе се употребат.

1. Во **процесот на анализа** на добиените информации во однос на веродостојната на информацијата од даден сервис или повеќе сервиси според табелата, добиените реултатите може да се искористат за да се прикаже средната веродостојност на информациите $\mathbf{V_E}$ кои се однесуваат за одредена проблематика.

2. Во **процес на планирање** на тоа кои информации да се собираат и очекување кој сервис ќе даде точна информација, исто така, се овозможува добиените резултати да се искористат во прикажување на средната веројатност за добивање на точна информација од активираните сервиси $\mathbf{(AV)_E}$.

Од Табела 3 може да заклучиме дека при користење на сервисот кој има најголема веројатност за добивање на очекувана точна информација, во процесот на планирање не може да се очекува дека и вредноста за веродостојноста на информацијата од истиот сервис ќе биде најголема во однос на другите сервиси.

За да се надмине овој проблем ќе се искористи начелото кое се користи во разузнавањето, а тоа е дека одредена информација мора да биде проверена од најмалку три извори на информации односно во нашиот случај, на три ралични сервиси. Сервисите кои ќе бидат употребени во процесот на планирање за собирање на информации да се изберат согласно критериумот за максимална вредност на веројатноста за добивање на точна информација.

Сепак, треба да се нагласи дека оптималното користење на сервисите во однос на веројатноста на добивање на точна информација од одреден сервис и веродостојноста на истата како краен продукт во процесот на анализа на информации, не коренспондира со добивање на максимални вредности и по двата параметра.

ГЛАВА 7

РАЗВОЈ НА МЕТРИКИ ЗА РАСПОЛОЖЛИВОСТ, ВЕРОДОСТОЈНОСТ И ВРЕМЕ ЗА ОДЗИВ НА СЕРВИСИТЕ ВО ИСР

Моделот за информацискиот систем за разузнавање дава придонес во јакнење на Националната безбедност на државата и исто така придонесува во јакнење на довербата на луѓето во современите општевства, кои се базираат на користење на современата информациско – комуникациска технологија во секојдневието.

СОА е технолошки пристап кон дизајнирање на информациските системи, каде што примарна цел е да се искорити развојот и достигнувањето на ИТ во бизнис процесите на начин на кој ќе се оствари поголема ефикасност, Но, исто така постојат дилеми дека со СОА ќе се решат голем број на технички проблеми и ќе се искористат придобивките ([73], [106], [107]). СОА претставува апстрактен концепт "service", каде сервисот е технологија - независна структура која го поедноставува процесот на слаба споеност (*engl.* loose coupling) и обезбедува основа за создавање компонентни (модуларни, отворени) архитектури ([108], [103], [109]).

„Quality of service (QoS)“ претставува карактеристика на сервисите преку која се утврдуваат одредени параметри на сервисите ([110]). Без разлика дали станува збор за веб сервиси или сервиси кои се дел од одреден информациски систем, параметрите за „QoS“ играат значајна улога. Параметрите за „QoS“ создаваат кај корисниците доверба и сигурност за користење на сервисите. Корисниците на сервисите посакуваат користење на сервиси кои искуствено функционирале без проблеми, како на пример кратко време на чекање, висока веродостојност и можност за успешно користење на сервисите.

Создавање на метрика и процес за мерење во секоја метрика мора да биде добро дефиниран, со цел клиентот и провајдерот да ја разберат.

Процесот за мерење на секоја метрика од „QoS“ треба да разработува ([111]):

- што да се мери (збирност (engl aggregates) или процентуалност);
- како да се мери (фрекфенција, интервали и алатки);
- кој да мери (сервис провајдерите или надворешните независни агенти);
- каде да се изврши мерењето (на крајот на мрежата, клиентот или пристапната точка на сервисот (*engl.* web service access point)

Исто така чинењето на веб сервисот (*engl.*Web service’s cost) е поврзано со неговиот квалитет. Побрзите, доверливите и безбедни сервиси би требало да бидат поскапи, но исто така без разлика на нивните перформанси, тие треба да бидат во согласност со целите за „QoS (Quality of service)“ или „service-level agreements (SLAs)“.

„QoS“ пошироко може да биде категоризиран во три категории: перформанси, зависност и безбедност. Во поглавјето се разработени параметри кои спаѓаат во првите две категории. Од првата категорија за параметрите на перформансите ќе се разработува време на одзив на сервисите, а за втората категорија за параметрите на зависност ќе се разработува расположливост на сервисот (*engl.*availability) и веродостојност (*engl.* reliability).

Поглавјето дава придонес во создавање на метрики за одредување на просечното време за одзив на сервисите од кои е составен информацискиот систем за разузнавање, после креирано барање од корисниците за одредена информација. Исто така, во поглавјето ќе бидат креирани метрики за раположливост на сервисите (*engl.* service availability) во однос на нивната искористливост за крајните корисници. Креирање на метрики за проценување на веродостојноста на информацијата (*engl.* service reliability assessment) е потребно важно бидејќи во трудот се разработува информациски систем за разузнавање.

7.1 Преглед на истражувања поврзани со поглавјето

Во ([110]) е претставена селекцијата за користење на веб сервиси врз основа на „QoS (*engl.* QoS based Web Service Selection)“. „QoS“ игра значајна улога бидејќи клиентите сакаат да употребуваат сервиси кои ќе одговорат на нивните барања. Селектирањето на веб сервисите е базирано на статусот кој е пресметан со оценките доделени од корисникот за секој веб сервис. Оценките самостојно не може да го опишат квалитетот на веб сервисот, па поради тоа треба да бидат земени во предвид други „QoS“ параметри. Во трудот се разработени седум параметри за „QoS“ и тоа извршно време (*engl.*execution time), време на одзив (*engl.* response time), пропусност (*engl.*throughput), мерливост (*engl.*scalability), „reputation“, достапност (*engl.* accessibility) и расположливост (*engl.*availability). Целта на концептот е да се обезбеди селекцијата за користење на веб сервиси врз основа на „QoS (*engl.* QoS based Semantic Web Service Selection)“. Концептот се состои од четири компоненти „OWL-S converter“, „Semantic Repository“, „QoS Broker“ и „Matchmaker“. Секоја од компонентите има своја функција.

Во ([112]) е предложено решение за моделирање на закон на распределба на веројатност (*engl.* probability density function (PDF)) на „QoS“ од веб сервиси „(QoWS)“ базирано на непараметарски статистички методи (*engl.* non-parametric statistical method). Математичките формули се дизајнирани за пресметување на „QoS“ дистрибуцијата на сервисните композиции „(QoCS)“. Експериментот е направен за да прикаже дека „QoWS“ моделираното решение е поточно отколку постоечките методи. Прецизна проценка на „PDF“ може да се добие за „QoCS“, доколку „PDF“ за компонентите од „QoWS“ се моделирани со предложениот метод.

Во ([113]), веб сервисите дозволуваат програмите да достават упит на други програми преку интернет со отворени протоколи и стандарди. Многу традицинални веб страни, вклучувајќи ги популарните машини за пребарување како „Google“ или продавниците за книги како „Amazon.com“, ја подобруваат интеракција со користење на „Web service APIs“. Единечни интернет апликации може да вовлекуваат многу различни сервиси, како на пример, метапребарувачката машина „WebSifter“ користи различни он-лајн онтологии за да го креира корисничкото барање како поразбирлив упит и потоа да го препрати истиот упит на различни машини за пребарување (*engl.* search engines) паралелно. Ваквите апликации се наречени композитни веб сервиси. Тежиште во трудот е дадено на влијанието на бавните сервиси врз вкупното време за одговор за дадена трансакција која се изведува со паралелна работа на повеќе веб сервиси.

Во ([114]) сервисно ориентираната архитектура се појавува како решение за креирање на апликации составени од сервиси со лабави врски. Како и да е, проблем со COA се нејзините карактеристиките, поради лабавите врски и хетерогената природа на решението. За практично и пошироко искористување на COA во апликациите кои се

развиваат потребно е, проблемот со карактеристиките да биде надминат. Поради тоа треба да се мери колку се ниски перформансите и да се анализира каде и зошто се појавува проблемот. Предуслов за претходно наведеното е дефинирање на јасни метрики за мерење на перформансите на сервисите. Под јасно дефинирана метрика, се подразбира метрика која е прецизна и доволно практична за ефикасно одредување на причината која го предизвикува проблемот за перфомансисте (карактеристките).

Моменталните истражувања за перформансите на сервисите се недоволно прецизни за да бидат искористени за ефективни дијагнози кои се однесуваат на карактеристиките на СОА. Како резултат, трудот предлага сет од прецизни и практични метрики за одредување на перформансите на сервисите. Истите метрики се искористени во „Hotel Reservation Service“, при што е прикажана апликативноста и корисноста од метриките.

7.2 Состојби на сервисно ориентиран информациски систем

Генерално, секој информациски систем кој е сервисно ориентиран, односно е базиран на сервисно ориентираната архитектура, зависи од состојбата на сервисите во одреден момент.

Под терминот состојба на сервисите ќе дефинираме активноста на сервисот при доставен упит од страна на клиентот за користење на сервисот. Така што, потребно е да се воведе величина која ќе ја одредува активноста на сервисот. Доколку сервисот е активен ќе воведеме величина “1“, доколу не е активен воведуваме величина “0“.

Доколку претходно наведеното го искористиме за состојба на сервисите (Табела 4), тогаш ја имаме следната табела:

Табела 4. Состојба на сервисот во ИСР

Активност	**Состојба на сервисот**
1	сервисот е во активна состојба
0	сервисот не е во актвна состојба

При одреден упит од клиентот за користење на даден сервис од ИСР, доколку имаме одзив на сервисот, тогаш утврдуваме дека сервисот се наоѓа во активна состојба и има активност “1“. Доколку, сервисот не даде одзив по доставениот упит од клиентот, тогаш следи заклучокот дека сервисот е во неактивна состојба и има активност “0“.

Бројот на можните состојби на информацискиот систем кој е сервисно ориентиран, без разлика каде е имплементиран и за што е наменет, зависи од состојбата на секој сервис, кој е составна компонента на информацискиот систем.

Ако n е вкупниот број на сервиси во информацискиот систем, тогаш бројот на состојби на информацискиот систем е:

$$\overline{V}_n^2 = 2^n \tag{7.1}$$

n – вкупен број на сервиси во информацискиот систем

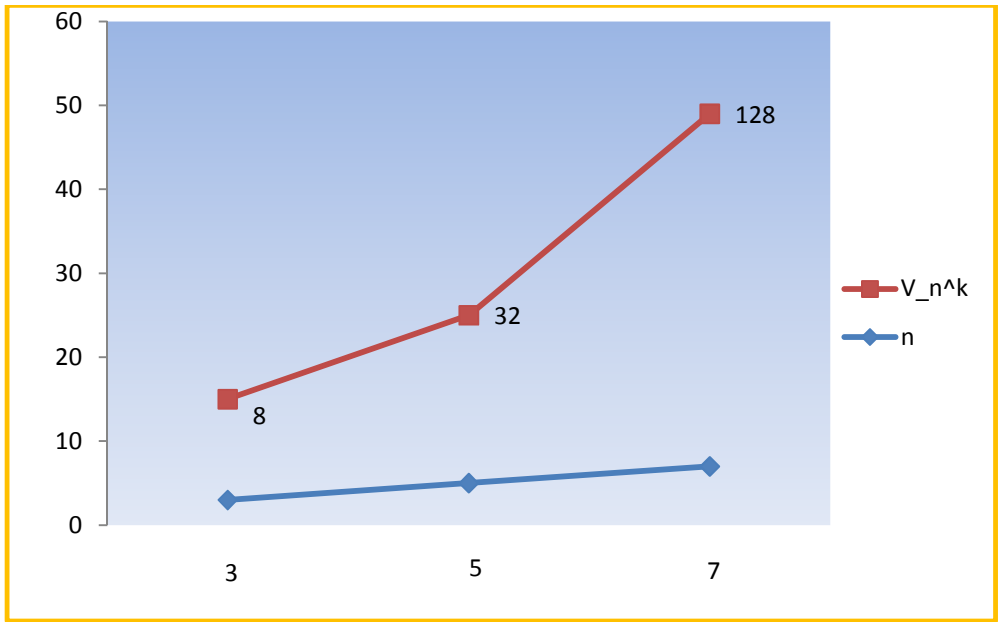
Ако разработиме одреден пример за информациски систем со различен број на сервиси, кои може да бидат во две состојби [0,1], односно активна и неактивна, и искористување на (7.1) имаме следно:

$$n = 3; \qquad V_3^2 = 2^3 = 8$$

$$n = 5; \qquad V_5^2 = 2^5 = 32$$

$$n = 7; \qquad V_7^2 = 2^7 = 128$$

Со цел подобра презентација на добиените резултати од наведениот пример и изнесување на заклучок за бројот на состојбите на информацискиот систем, ќе го воведеме следниот графичко приказ (Слика 33):



Слика 33. Графички приказ на зависноста на бројот на состојбите на информацискиот систем од бројот на сервиси

Врз основа на разработениот пример и графичкиот приказ може да заклучиме дека колку бројот на сервисите се зголемува, толку побрзо се зголемува бројот на можните состојби во кои информацискиот систем може да биде во одреден момент во зависност од одреден упит на клиентот.

Важноста од определување на бројот на состојбите на инфромацискиот систем, се темели на влијанието од наведената метрика врз вкупниот „QoS“ на информацискиот систем.

Со цел подобро презентирање на наведеното, може да се напомене дека со знаење на бројот на состојбите, може полесно да се одреди веројатноста за добивање на информација од одреден сервисно ориентиран инфромациски систем. Констатацијата се темели на метриката за состојбите на одреден систем, бидејќи колку е поголем бројот на сервисите во информациските системи, толку е поголем бројот на состојбите на системот, а со самото тоа и веројатноста за добивање на информација од системот.

Во ист контекст, доколку го разработиме времето за одзив на сервисот, влијанието на метриката за бројот на состојбите се однесува на пресметување на просечното време за одзив на сервисот. Доколку имаме одреден упит од клиент за дадена информација, тогаш просечното време за одзив на сервисот за добивање на информацијата од сервисно-

ориентираниот информациски систем, може директно да зависи од бројот на состојбите во кои може да се најде системот.

7.3 Расположливост на сервисите

Расположливост е карактеристика на сервисот без разлика дали тој е активен или достапен за користење по доставено барање во одреден момент во однос на неговата веродостојност. За фреквентно користените сервиси, со мали вредности за периодот на опсервација можно е поточна апроксимација на расположливост на сервисите (*engl.*service availability) ([115]).

Да разработиме информациски систем кој е сервисно ориентиран, при тоа истиот е составен од n сервиси, кои меѓусебно се независни. Секој од сервисите може да биде активен или неактивен при доставено барање за негово користење, независно од останатите. Нека со p ја означиме веројатноста дека сервисот ќе биде достапен при даден упит од страна на клиентот, со 1-p ќе ја означиме веројатноста дека сервисот нема да биде достапен. Ќе сметаме дека информацијата од системот е комплетна, ако од n сервиси функционираат или се достапни x. Ако бројот на сервисите кои функционираат е ≤ x-1, тогаш информацијата не е комплетна.

Нека X е случајна променлива која го означува бројот на достапни сервиси. Согласно претходното, X има биномна распределба, т.е. $X \sim B(n,p)$, па

$$f(x) = P(X = x) = \binom{n}{x} p^x (1-p)^{n-x}, \quad x \in \{0,1 \dots, n\}. \tag{7.2}$$

Математичкото очекување на случајната променлива X е:

$$E(X) = np \tag{7.3}$$

$E(X)$ – очекуван број на сервиси кои ќе бидат достапни при одреден упит од клиентот
n – вкупен број на сервиси
p – веројатност дека еден сервис ќе биде достапен при одреден упит од информацискиот систем

Условот ќе биде исполнет не само кога бројот на достапните сервиси е еднаков на x, туку и кога тој број е поголем од x. Така што веројатноста за условот да биде задоволен е:

$$P(X \geq x) = \sum_{i=x}^{n} P(X = i) = \sum_{i=x}^{n} \binom{n}{i} p^i (1-p)^{n-i} \tag{7.4}$$

Исто така равенката (7.4) може да се напише и во следниот облик:

$$P(X \geq x) = 1 - P\{X < x\} = 1 - \sum_{i=0}^{x-1} \binom{n}{i} p^i (1-p)^{n-i} \tag{7.5}$$

Функцијата $F(x) = P\{X < x\}$ е функција на распределба на случајната променлива X.

Пресметувањето на очекуваниот број на сервиси кои нема да бидат достапни при одреден упит, се темели на претходно наведената равенка. Законот на распределба на случајната променлива Y:број на недостапни сервиси, е определен со:

$$f(y) = P(Y = y) = \binom{n}{y}(1-p)^y p^{n-y},\ y \in \{0,1,2,\ldots,n\} \quad (7.6)$$

Y- случајна променлива која го претставува бројот на недостапните сервиси
y – број на недостапни сервиси за $y = 0,1,2,3 \ldots \ldots \ldots, n$

Значи, Y~B(n, 1-p), па за нејзиното математичко очекување се добива :

$$E(Y) = n(1-p) \quad (7.7)$$

$E(Y)$ – очекуван број на сервиси кои ќе бидат недостапни при одреден упит од клиентот
n – вкупен број на сервиси
$1 - p$ – веројатност дека еден сервис ќе биде недостапен при одреден упит од информацискиот систем

Очекуваниот број на достапни сервиси (7.3) и очекуван број (7.7) на недостапни сервиси, може да се употребат за воспоставување на критериум или одредена граница (*engl.*threshold) за добивање на веродостојна разузнавачка информација од информацискиот систем за разузнавање.

Со цел подобро презентирање на наведеното, ќе воведеме две зони (зелена и црвена), според очекуваните вредности на бројот на недостапни и достапни сервиси (Табела 5). Доколку имаме очекуван број на достапни сервиси (според (7.3)) кој е еднаков или поголем од нивото на воспоставената граница, тогаш веројатноста за добивање на веродостојна информација од сервисно ориентираниот информациски систем ќе биде претставена со зелена зона. Доколку имаме помали вредности за очекуваниот број од (7.3), односно поголеми вредности за очекуваниот број на недостапни сервиси од (7.7), тогаш ќе ја користиме црвената зона.

Табела 5. Очекуван број на достапни со соодветни зони

Очекувани броеви	Зони
очекуван број на достапни сервиси E(X)	
очекуван број на недостапни сервиси E(Y)	

Доколку се разработи информациски систем за разузнавање со одреден број на сервиси, без разлика на тоа за какви сервиси станува збор, од особен интерес за добивање на разузнавачка информација ќе биде вредноста на математичкото очекување од (7.3). Како пример за сервиси во информацискиот систем за разузнавање може да се наведат претходно споменатите разузнавачки дисциплини, кои за собирање, обработка и дисиминација на информациите користат одредени технички средства. Технички средства кои се користат се следните: видео камери, беспилотни летала (*engl.* UAVs), беспосадни копнени возила (*engl.* UGVs), разни видови на воздухоплови, технички средства за мерење и обележување итн. Во најголемиот број на случаи, овие технички средства се поврзуваат со одреден хардвер и софтвер.

Доколку имаме објект кој е од разузнавачки интерес, во зависност од тоа кои сервиси се содржат во инфромацискиот систем за разузнавање, нивната функционалност и намена, можеме да одредиме кои информации ќе може да се собираат за објектот. На пример, видео камерите, може да се користат за добивање на информација за одредено лице, возило и други објекти кои се од разузнавачки интерес, потоа беспилотните летала се користат за добивање на информации за терен, одредена непријателска зона, терористички групи итн.

Примената на очекуваната вредност од (7.3) во сервисно ориентиран информациски систем кој се состои од две камери и едно беспилотно летало, ќе се однесува на евалуација на веројатноста за бројот на достапни сервиси на целокупниот информациски систем. Информацијата за објектот од разузнавачки интерес може да се добие од трите наведени сервиси.

Нека секој сервис е достапен со веројатност 1/3. Ќе сметаме дека информацијата е комплетна, ако два сервиса се достапни. Тоа значи дека информацискиот систем ќе функционира (ќе биде во зелена зона) ако веројатноста за достапност на сервисите е ≥ 7/27. Имено,

$$P(X \geq 2) = P(X = 2) + P(X = 3) = \binom{3}{2}\left(\frac{1}{3}\right)^2\left(\frac{2}{3}\right)^1 + \binom{3}{3}\left(\frac{1}{3}\right)^3\left(\frac{2}{3}\right)^0 = \frac{7}{27}.$$

Во спротивно системот е во црвена зона.

7.3.1 Користење на Маркови модели за анализа на расположливоста на сервисите

Недостапноста на сервисите во сервисно ориентиран информациски систем се поврзува со различните типови на грешки, откажувања со работа и планирани отстранувања на мрежните компоненти, потоа различни компоненти на страната на сервис провајдерот и компоненти за пристап на корисникот ([117]). За анализа на сервисно-ориентираните информациски системи во однос на расположливост и веродостојност на сервисите најпогодни се Марковите модели. Претпоставката дека во одреден временски момент системот или сервисот (доколку се разгледува како систем), се наоѓа во една од конечниот број на состојби и сервисите се недостапни според експоненцијална распределба, овозможува примена на Марковите модели за одредување на раположливост и веродостојност на сервисите. Во зависност од карактерот на овие величини – дискретен или непрекинат тип – Марковите модели може да имаат различни облици (Маркови вериги или Маркови процеси). Од аспект на одредување на расположливост и веродостојност на системот, од практично значење се Марковите процеси каде состојбата

на системот X(t) е случајна променлива од дискретен тип, со непрекинато параметарско множество.

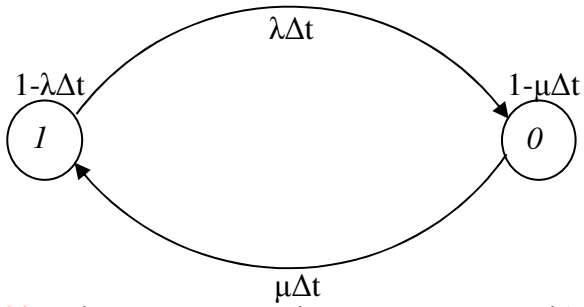
За анализа на расположливоста на сервисот ќе ги користиме хомогените Маркови модели со конечен број на состојби (Слика 34). Пример за вакви модели се процесите на умирање и раѓање, кои се користат како модел за опишување на разни природни, технички и општествени системи и процеси.

Нека X(t) е случаен процес кој прима вредности од множевството {0,1} и достапност на сервисот во време t, т.е.

$$x = \begin{cases} 0, \text{ако сервисот не е достапен во време t} \\ 1, \text{ако сервисот е достапен во време t} \end{cases}$$

Нека λ е интензитет на премин од состојба 1 во состојба 0, а μ е интензитет на премин од состојба 0 во состојба 1.

Случај I



Слика 34. Дијаграм на транзиција (преоѓање) на состојбите

Веројатноста $P_1(t + \Delta t)$ во момент t+Δt (за мало $\Delta t > 0$), сервисот да се најде во состојба 1 се определува на следниот начин:

- во моментот t, сервисот бил во состојба 1 и остнал во истата состојба (веројатноста на овој настан е $P_1(t)\,(1 - \lambda\Delta t)$),
- во момент t, сервисот бил во состојба 0 и од неа за време Δt, поминал во состојба 1 (веројатноста е $P_0(t)\,\mu\Delta t$)

Оттука,

$$P_1(t + \Delta t) = P_1(t)\,(1 - \lambda\Delta t) + P_0(t)\mu\Delta t \qquad (7.8)$$

Сервисот во момент t+Δt ќе се најде во состојба 0, во следните случаи:

- во моментот t, сервисот е во состојба 1 и за време Δt поминува од состојба 1 во состојба 0 (веројатноста на овој настан е $P_1(t)\lambda\Delta t$),
- во момент t, сервисот бил во состојба 0 и за време Δt, не поминува во друга состојба (веројатноста е $P_0(t)(1 - \mu\Delta t)$)

Оттука,

$$\mathrm{P}_0\,(\mathrm{t}+\Delta\mathrm{t}) = \mathrm{P}_1\,(\mathrm{t})\,(\lambda\Delta\mathrm{t}) + \mathrm{P}_0\,(\mathrm{t})(1-\mu\Delta\mathrm{t}) \tag{7.9}$$

Понатаму потребно е да се решаваат да се изразат $\mathrm{P}_1(t)$ и $\mathrm{P}_0\,(t)$.
*) Од (7.8) се добива:

$$\mathrm{P}_1\,(t+\Delta t) = \mathrm{P}_1\,(t) - \lambda\Delta t\mathrm{P}_1\,(t) + \mathrm{P}_0\,(t)\mu\Delta t$$
$$\mathrm{P}_1\,(t+\Delta t) - \mathrm{P}_1\,(t) = (\mu\mathrm{P}_0\,(t) - \lambda\mathrm{P}_1\,(t))\Delta t$$
$$\frac{\mathrm{P}_1(t+\Delta t) - \mathrm{P}_1\,(t)}{\Delta t} = \mu\mathrm{P}_0\,(t) - \lambda\mathrm{P}_1\,(t)$$

Нека допуштиме $\Delta t \to 0$, тогаш:

$$\lim_{\Delta t\to 0}\frac{\mathrm{P}_1\,(t+\Delta t) - \mathrm{P}_1\,(t)}{\Delta t} = \lim_{\Delta t\to 0}(\,\mu\mathrm{P}_0\,(t) - \lambda\mathrm{P}_1\,(t)) \tag{7.10}$$

односно

$$\frac{\mathrm{dP}_1\,(t)}{\mathrm{d}t} = \mu\mathrm{P}_0\,(t) - \lambda\mathrm{P}_1\,(t)$$

при што со примена на Лапласова трансформација, по таблица за $\frac{\mathrm{d}f(t)}{\mathrm{d}t} = sL\,[f(\mathrm{t})] - f(0)$ и замена во (7.10), следува:

$$\mathrm{sL}[\mathrm{P}_1\,(\mathrm{t})] - \mathrm{P}_1\,(0) = \mathrm{L}\mu\mathrm{P}_0\,(t) - \mathrm{L}\lambda\mathrm{P}_1\,(t)$$
$$\mathrm{sL}[\mathrm{P}_1\,(\mathrm{t})] - \mathrm{L}\mu\mathrm{P}_0\,(t) + \mathrm{L}\lambda\mathrm{P}_1\,(t) = \mathrm{P}_1\,(0)$$
$$\mathrm{L}[\mathrm{s}[\mathrm{P}_1\,(\mathrm{t})] + \lambda\mathrm{P}_1\,(t) - \mu\mathrm{P}_0\,(t)] = \mathrm{P}_1\,(0)$$

$$\mathrm{L}[(\mathrm{s}+\lambda)[\mathrm{P}_1\,(t)] - \mu L[\mathrm{P}_0\,(t)] = \mathrm{P}_1\,(0)$$

$$(\mathrm{s}+\lambda)\mathrm{L}[\mathrm{P}_1\,(t)] - \mu L[\mathrm{P}_0\,(t)] = \mathrm{P}_1\,(0) \tag{7.11}$$

*) Од (7.9) се добива:

$$\mathrm{P}_0\,(t+\Delta t) = \mathrm{P}_1\,(t)\,\lambda\Delta t + \mathrm{P}_0\,(t) - \mathrm{P}_0\,(t)\mu\Delta t$$
$$\mathrm{P}_0\,(t+\Delta t) - \mathrm{P}_0\,(t) = \mathrm{P}_1\,(t)\,\lambda\Delta t - \mathrm{P}_0\,(t)\mu\Delta t$$
$$\mathrm{P}_0\,(t+\Delta t) - \mathrm{P}_0\,(t) = (\mathrm{P}_1\,(t)\,\lambda - \mathrm{P}_0\,(t)\mu)\Delta t$$
$$\frac{\mathrm{P}_0\,(t+\Delta t) - \mathrm{P}_0\,(t)}{\Delta t} = \lambda\mathrm{P}_1\,(t)\; - \mu\mathrm{P}_0\,(t)$$

Ако $\Delta t \to 0$, добиваме:

$$\lim_{\Delta t\to 0}\frac{\mathrm{P}_0\,(t+\Delta t) - \mathrm{P}_0\,(t)}{\Delta t} = \lim_{\Delta t\to 0}(\lambda\mathrm{P}_1\,(t)\; - \mu\mathrm{P}_1\,(t)) \tag{7.12}$$

односно

$$\frac{\mathrm{dP_0\,(t)}}{\mathrm{dt}} = \lambda \mathrm{P_1}\,(t)\; - \mu \mathrm{P_0}\,(t)$$

при што со примена на Лапласова трансформација, по таблица за $\frac{\mathrm{d}f(t)}{\mathrm{d}t} \rightarrow sL\,[f(\mathrm{t})] - f(0)$ и замена во(7.12), следува:

$$\mathrm{sL}[\mathrm{P_0\,(t)}] - \mathrm{P_0\,(0)} - \mathrm{L}\lambda \mathrm{P_1}\,(t) + \mathrm{L}\mu \mathrm{P_0}\,(t) = 0$$
$$\mathrm{sL}[\mathrm{P_0\,(t)}] - \;\mathrm{L}\lambda \mathrm{P_1}\,(t) + \mathrm{L}\mu \mathrm{P_0}\,(t) = \mathrm{P_0\,(0)}$$

$$-\mathrm{L}\lambda \mathrm{P_1}\,(t) + \mathrm{L}(\mathrm{s} + \mu)[\mathrm{P_0\,(t)}] \;= \mathrm{P_0\,(0)}$$
$$-\lambda \mathrm{LP_1}\,(t) + (\mathrm{s} + \mu)\mathrm{L}[\mathrm{P_0\,(t)}] \;= \mathrm{P_0\,(0)} \qquad (7.13)$$

За да се продолжи со понатамошно решавање на равенките за веројатностите во состојбите на сервисот 1 и 0, потребно е да се воведат матрици, при што од (7.11) и (7.13), следува:

$$\begin{bmatrix} \mathrm{s} + \lambda & -\mu \\ -\lambda & s + \mu \end{bmatrix} \begin{bmatrix} \mathrm{L}[\mathrm{P_1\,(t)}] \\ \mathrm{L}[\mathrm{P_0\,(t)}] \end{bmatrix} = \begin{bmatrix} \mathrm{P_1\,(0)} \\ \mathrm{P_0\,(0)} \end{bmatrix}$$

или

$$[\mathrm{L}[\mathrm{P_1\,(t)}]\;\mathrm{L}[\mathrm{P_0\,(t)}]] \begin{bmatrix} s + \lambda & -\mu \\ -\lambda & \mathrm{s} + \mu \end{bmatrix} = [\mathrm{P_1\,(0)P_0\,(0)}] \qquad (7.14)$$

Ги воведуваме следните ознаки:

$$\mathrm{T} = [\mathrm{L}[\mathrm{P_1\,(t)}]\;\mathrm{L}[\mathrm{P_0\,(t)}]] \qquad \mathrm{A} = \begin{bmatrix} s + \lambda & -\mu \\ -\lambda & \mathrm{s} + \mu \end{bmatrix} \qquad \mathrm{P} = [\mathrm{P_1\,(0)P_0\,(0)}]$$

Со замена во (7.17), се добива:

$$\mathrm{TA} = \mathrm{P} \qquad (7.15)$$

и со множење од десно на двете страни на изразот (7.15) со инверзна квадратна матрица $\mathrm{A^{-1}}$, се добива:

$$\mathrm{TA} = \mathrm{P} \qquad /\mathrm{A^{-1}}$$
$$\mathrm{TAA^{-1}} = \mathrm{PA^{-1}}$$
$$\mathrm{T} = \mathrm{PA^{-1}} \qquad (7.16)$$

За одредување на квадратната матрица $\mathrm{A^{-1}}$, имаме:

$$\mathrm{A^{-1}} = \frac{adj\;\mathrm{A}}{\det\;\mathrm{A}} \qquad \text{односно} \qquad \mathrm{A^{-1}} = \frac{1}{\det\;\mathrm{A}}\,\widetilde{\mathrm{A^*}}$$

$$adj\ \mathrm{A} = \begin{bmatrix} s+\mu & \mu \\ \lambda & \mathrm{s}+\lambda \end{bmatrix}$$

$$\det\ \mathrm{A} = \big((\mathrm{s}+\lambda)(\mathrm{s}+\mu)\big) - \big((-\lambda)(-\mu)\big) = \mathrm{s}^2 + \mathrm{s}\mu + \mathrm{s}\lambda + \lambda\mu - \lambda\mu$$

$$\det\ \mathrm{A} = \mathrm{s}(\mathrm{s}+\mu+\lambda)$$

Со замена за $\det\ \mathrm{A}$ и $adj\ \mathrm{A}$ во A^{-1}, следува:

$$\mathrm{A}^{-1} = \frac{1}{\mathrm{s}(\mathrm{s}+\mu+\lambda)} \begin{bmatrix} s+\mu & \mu \\ \lambda & \mathrm{s}+\lambda \end{bmatrix}$$

$$\mathrm{A}^{-1} = \begin{bmatrix} \dfrac{s+\mu}{\mathrm{s}(\mathrm{s}+\mu+\lambda)} & \dfrac{\mu}{\mathrm{s}(\mathrm{s}+\mu+\lambda)} \\ \dfrac{\lambda}{\mathrm{s}(\mathrm{s}+\mu+\lambda)} & \dfrac{\mathrm{S}+\lambda}{s(\mathrm{s}+\mu+\lambda)} \end{bmatrix} \tag{7.17}$$

Со решавање на матричната равенка (7.16), се добиваат решенија за $\mathrm{L}[\mathrm{P}_1(\mathrm{t})]$ и $\mathrm{L}[\mathrm{P}_0(\mathrm{t})]$, во форма на Лапласова трансформација за бараните веројатности.

Доколку се претпостави дека на почетокот немало настани, односно сервисот бил активен и се наоѓал во состојба "1", следува дека $\mathrm{P}_1(0) = 1$ и $\mathrm{P}_0(0) = 0$, тогаш имаме:

$$[1\ 0] \begin{bmatrix} \dfrac{\mathrm{s}+\mu}{\mathrm{s}(\mathrm{s}+\mu+\lambda)} & \dfrac{\lambda}{\mathrm{s}(\mathrm{s}+\mu+\lambda)} \\ \dfrac{\mu}{\mathrm{s}(\mathrm{s}+\mu+\lambda)} & \dfrac{\mathrm{s}+\lambda}{\mathrm{s}(\mathrm{s}+\mu+\lambda)} \end{bmatrix} = [\mathrm{L}[\mathrm{P}_1(\mathrm{t})]\ \mathrm{L}[\mathrm{P}_0(\mathrm{t})]$$

$$\mathrm{L}[\mathrm{P}_1(\mathrm{t}) = \frac{\mathrm{s}+\mu}{\mathrm{s}(\mathrm{s}+\mu+\lambda)} \tag{7.18}$$

$$\mathrm{L}[\mathrm{P}_0(\mathrm{t})] = \frac{\lambda}{\mathrm{s}(\mathrm{s}+\mu+\lambda)} \tag{7.19}$$

Со разложување на коефициенти, за (7.18 да се измени), следи:

$$\mathrm{L}[\mathrm{P}_1(\mathrm{t})] = \frac{\mathrm{K}_1}{\mathrm{s}} + \frac{\mathrm{K}_2}{(\mathrm{s}+\mu+\lambda)}$$

$$\mathrm{K}_1 = \mathrm{sL}[\mathrm{P}_1(\mathrm{t})|_{\mathrm{s}=0} = \frac{\mathrm{s}+\mu}{\mathrm{s}+\mu+\lambda} = \frac{\mu}{\mu+\lambda} \qquad \Rightarrow \mathrm{K}_1 = \frac{\mu}{\mu+\lambda}$$

$$\mathrm{K}_2 = (\mathrm{s}+\mu+\lambda)\mathrm{L}[\mathrm{P}_1(\mathrm{t})|_{s=-\mu-\lambda} = \frac{\mathrm{s}+\mu}{\mathrm{s}} = \frac{-\mu-\lambda+\mu}{-\mu-\lambda} \qquad \Rightarrow \mathrm{K}_2 = \frac{\lambda}{\mu+\lambda}$$

Со замена на вредностите за K_1 и K_2 во (7.18):

$$L[P_1(t)] = \frac{\frac{\mu}{\mu+\lambda}}{s} + \frac{\frac{\lambda}{\mu+\lambda}}{(s+\mu+\lambda)} = \frac{\mu}{s(\mu+\lambda)} + \frac{\lambda}{(\mu+\lambda)(s+\mu+\lambda)}$$

$$L[P_1(t) = \frac{1}{\mu+\lambda}\left(\frac{\mu}{s} + \frac{\lambda}{s+\mu+\lambda}\right) \tag{7.20}$$

Со разложување на коефициенти, за (7.19), следи:

$$L[P_0(t)] = \frac{\lambda}{s(s+\mu+\lambda)} = \frac{K_1}{s} + \frac{K_2}{(s+\mu+\lambda)}$$

$$K_1 = sL[P_0(t)|_{S=0} = \frac{\lambda}{s+\mu+\lambda} = \frac{\lambda}{\mu+\lambda} \quad \Rightarrow K_1 = \frac{\lambda}{\mu+\lambda}$$

$$K_2 = (s+\mu+\lambda)L[P_0(t)|_{s=-\mu-\lambda} = \frac{\lambda}{s} = -\frac{\lambda}{\mu+\lambda} \quad \Rightarrow K_2 = -\frac{\lambda}{\mu+\lambda}$$

Со замена на вредностите за K_1 и K_2 во (7.19):

$$L[P_0(t)] = \frac{\frac{\lambda}{\mu+\lambda}}{s} - \frac{\frac{\lambda}{\mu+\lambda}}{(s+\mu+\lambda)} = \frac{\lambda}{s(\mu+\lambda)} - \frac{\lambda}{(\mu+\lambda)(s+\mu+\lambda)}$$

$$L[P_0(t)] = \frac{\lambda}{\mu+\lambda}\left(\frac{1}{s} - \frac{1}{s+\mu+\lambda}\right) \tag{7.21}$$

Со наоѓање на инверзна Лапалсова трансформација, се добиваат следните равенки за веројатностите $P_0(t)$ и $P_1(t)$:

*) од таблицата за Лапласова трансформација се добиваат следните замени:

$$L[1] = \frac{1}{s} \qquad L[e^{bt}] = \frac{1}{s-b} \qquad L[e^{-bt}] = \frac{1}{s+b}$$

*.1) Со замена во табличните вредности од Лапласовата трансформација во (7.20)

$$L[P_1(t)] = \frac{1}{\mu+\lambda}\left(\frac{\mu}{s} + \frac{\lambda}{s+\mu+\lambda}\right) = \frac{1}{\mu+\lambda}\left(\mu\frac{1}{s} + \lambda\frac{1}{s+\mu+\lambda}\right)$$

$$P_1(t) = \frac{1}{\mu+\lambda}\left(\mu + \lambda e^{-(\mu+\lambda)t}\right)$$

$$P_1(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda}e^{-(\mu+\lambda)t} \tag{7.22}$$

*.2) Со замена во табличните вредности од Лапласовата трансформација во (7.21)

$$L[P_0(t) = \frac{\lambda}{\mu+\lambda}\left(\frac{1}{s} + \frac{1}{s+\mu+\lambda}\right)$$

$$P_0(t) = \frac{\lambda}{\mu+\lambda}\left(1 - e^{-(\mu+\lambda)t}\right) \tag{7.23}$$

Функцијата за расположливоста на сервисот во зависност од времето е:

$$A(t) = P_1(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda} e^{-(\mu+\lambda)t} \quad (7.24)$$

Бидејќи функцијата за расположливоста на сервисот е зависна од времето t, потребно е да се напомене дека сервисот ќе биде непрекинато достапен или активен за користење доколку $t \to \infty$. Во тој случај за функцијата за расположливоста на сервисот A(t), следува дека таа тежи кон константа, односно за A(t), ќе важи:

$$A = \lim_{t\to\infty} A(t) = \lim_{t\to\infty} P_1(t) = \frac{\mu}{\mu+\lambda} \quad (7.25)$$

7.3.1.1 Пример 1

Доколку имаме одреден сервис од сервисно ориентиран информациски систем и при тоа е потребно да се пресмета расположливоста на сервисите, исто така може да се искористат Марковите модели за поставување на почетните равенки, како и нивните зависности.

Ние ќе ја испитуваме расположливоста на сервисот во даден временски интервал од 0 до t, за информациски систем каде се примаат голем број на упити од најразлични клиенти. При тоа ќе ги користиме истите претпоставки кои беа наведени во претходната секција за интензитетите за достапност и недостапност на сервисот и случајните променливи.

Исто така, ќе претпоставиме дека сервисот може да се наоѓа во состојби кои ќе бидат моделирани со употреба на марковите модели.

Првата состојба на сервисот при одреден упит или повеќе упити од поголем број на клиенти во одреден момент t, ќе кореспондира на претпоставката дека сервисот е достапен или активен за користење од страна на корисниците. Таа состојба на сервисот ќе ја означиме со 1.

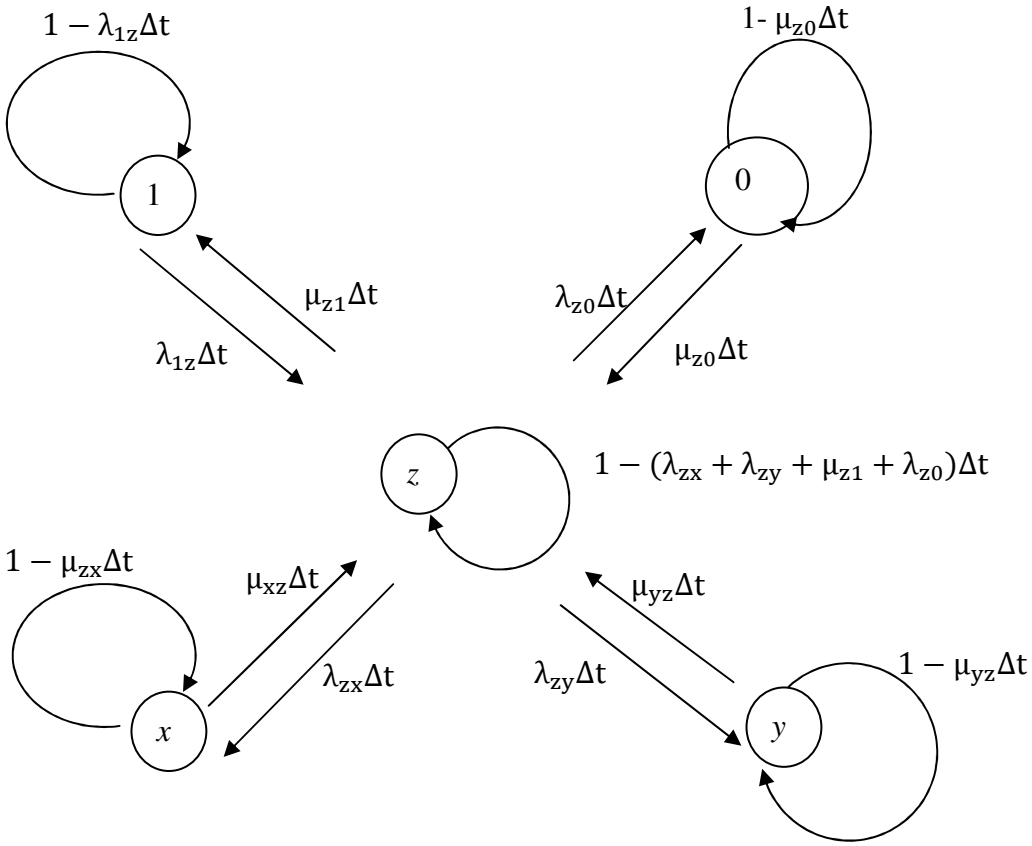
Доколку сервисот во одреден момент Δt премине во неактивна состојба, односно е недостапен за корисниците, тогаш тој преминува во неактивна состојба, која ќе ја означуваме со 0.

Двата случаи кои се однесуваат за состојбите на сервисот кога тој се наоѓа во состојба i и j се разработени во претходната секција.

За презентирање на расположливоста на сервисот во сервисно ориентираната архитектура, односно во информациските системи кои се базираат на СОА, потребно е да се воведат и други состојби кои подобро ќе го објаснат однесувањето на сервисите.

Состојбите кои ќе ги презентираме се оние во кои може да се најде сервисот во временски момент кога веројатноста за добивање на одговор од сервисот (*engl.* service response) е еднаква со веројатноста кога се очекува и недобивање на одговор од сервисот. Така да, ќе воведеме состојба z, која ќе се однесува на состојба на сервисот кога тој ќе го процесира упит од клиентите. Како резултат на преоѓање на системот во оваа состојба, тој понатаму може да продолжи во двете состојби со иста веројатност за добивање или недобивање на одговор од сервисот. Доколку имаме одговор од сервисот, тогаш тој ќе премине во состојба која ќе ја дефинираме со x. Доколку сервисот премине од состојбата z во состојба каде постои веројатноста за недобивање на одговор од сервисот, тогаш таа состојба во која се наоѓа сервисот ќе ја дефинираме како y.

Врз основа на претходно наведеното, состојбите низ кои сервисот може да се движи, односно транзицијата на состојбите, ќе се представи со следниот дијаграм (Слика 35):

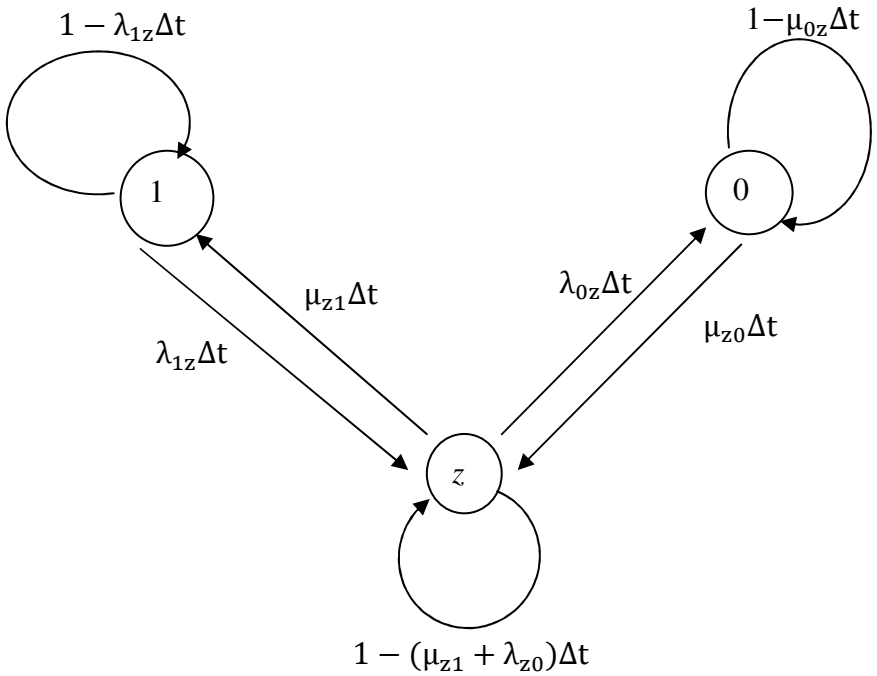


Слика 35. Дијаграм на транзиција (преоѓање) на состојбите

Бидејќи состојбата x е потполно идентична со состојба 1, односно сервисот по влегување во состојба z во даден временски интервал преминал во активна состојба, како резултат следува дека имаме преклопување на две исти состојби. Врз основа на наведената причина, состојбата x ќе се замени со 1.

Состојбата y е потполно идентична со состојбата 0, односно сервисот по влегување во состојба z во даден временски интервал излегува и преминува во неактивна состојба, односно станува недостапен за корисниците. Бидејќи се појавува преклопување на две исти состојби, состојбата y може да се замени со 0.

Заменувањето на состојбите овозможува упростување на дијаграмот на транзиција (Слика 36) и избегнување на креирање на комплексни равенства за понатамошно решавање на Марковите модели. Упростениот дијаграм на транзиција на состојбите ќе изгледа како по следното:



Слика 36. Дијаграм на транзиција (преоѓање) на состојбите

Понатаму потребно е да се изразат по $P_1(t)$, $P_z(t)$ и $P_0(t)$.

*) за $P_1(t+\Delta t)$, кога сервисот се наоѓа во состојба 1,

$$P_1(t+\Delta t) = (1-\lambda_{1z}\Delta t)P_1(t) + P_z(t)\mu_{z1}\Delta t$$

$$P_1(t+\Delta t) - P_1(t) = (\mu_{z1}P_z(t) - \lambda_{1z}P_1(t))\Delta t$$

$$\frac{P_1(t+\Delta t)-P_1(t)}{\Delta t} = (\mu_{z1}P_z(t) - \lambda_{1z}P_1(t))$$

Ако $\Delta t \to 0$, добиваме :

$$\lim_{\Delta t\to 0}\frac{P_1(t+\Delta t)-P_1(t)}{\Delta t} = \lim_{\Delta t\to 0}(\mu_{z1}P_z(t) - \lambda_{1z}P_1(t)) \qquad (7.26)$$

односно

$$\frac{dP_1(t)}{dt} = \mu_{z1}P_z(t) - \lambda_{1z}P_1(t)$$

при што со примена на Лапласова трансформација, по таблица за $\frac{df(t)}{dt} \to sL[f(t)] - f(0)$ и замена (7.26), следува:

$$Ls[P_1(t)] - P_1(0) = L\mu_{z1}P_z(t) - L\lambda_{1z}P_1(t)$$

$$Ls[P_1(t)] - L\mu_{z1}P_z(t) + L\lambda_{1z}P_1(t) = P_1(0)$$

$$L(s[P_1(t)] + L\lambda_{1z}P_1(t) - L\mu_{z1}P_z(t)) = P_1(0)$$

$$L(s + L\lambda_{1z})[P_1(t)] - L\mu_{z1}P_z(t) = P_1(0) \qquad (7.27)$$

*) за $P_z(t+\Delta t)$, кога сервисот се наоѓа во состојба "z",

$$P_z(t+\Delta t) = P_1(t)\,\lambda_{1z}\Delta t + P_z(t)(1-(\mu_{z1}+\lambda_{z0})\Delta t) + P_0(t)\mu_{z0}\Delta t$$
$$P_z(t+\Delta t) - P_z(t) = P_1(t)\,\lambda_{1z}\Delta t - P_z(t)(\mu_{z1}+\lambda_{z0})\Delta t + P_0(t)\mu_{z0}\Delta t$$
$$P_z(t+\Delta t) - P_z(t) = (P_1(t)\,\lambda_{1z} - P_z(t)(\mu_{z1}+\lambda_{z0}) + P_0(t)\mu_{z0})\Delta t$$

$$\frac{P_z(t+\Delta t) - P_z(t)}{\Delta t} = P_1(t)\,\lambda_{1z} - P_z(t)(\mu_{z1}+\lambda_{z0}) + P_0(t)\mu_{z0}$$

Ако $\Delta t \to 0$, се добива:

$$\lim_{\Delta t\to 0}\frac{P_z(t+\Delta t) - P_z(t)}{\Delta t} = \lim_{\Delta t\to 0}(P_1(t)\,\lambda_{1z} - P_z(t)(\mu_{z1}+\lambda_{z0}) + P_0(t)\mu_{z0}) \qquad (7.28)$$

односно

$$\frac{dP_z(t)}{dt} = (P_1(t)\,\lambda_{1z} - P_z(t)(\mu_{z1}+\lambda_{z0}) + P_0(t)\mu_{z0})$$

при што со примена на Лапласова трансформација и замена во (7.28), следува:

$$sL[P_z(t)] - L\lambda_{1z}P_1(t) + LP_z(t)(\mu_{z1}+\lambda_{z0}) - L\mu_{z0}P_0(t) = P_z(0)$$
$$sL[P_z(t)] - L\lambda_{1z}P_1(t) + LP_z(t)(\mu_{z1}+\lambda_{z0}) - L\mu_{z0}P_0(t) = P_z(0)$$
$$-L\lambda_{1z}P_1(t) + L(s+\mu_{z1}+\lambda_{z0})[P_z(t)] - L\mu_{z0}P_0(t) = P_z(0) \qquad (7.29)$$

*) за $P_0(t+\Delta t)$, кога сервисот се наоѓа во состојба "0",

$$P_0(t+\Delta t) = P_z(t)\,\lambda_{0z}\Delta t + P_0(t)(1-\mu_{0z}\Delta t)$$
$$P_0(t+\Delta t) - P_0(t) = P_z(t)\,\lambda_{0z}\Delta t - P_0(t)\mu_{0z}\Delta t$$
$$P_0(t+\Delta t) - P_0(t) = (P_z(t)\,\lambda_{0z} - P_0(t)\mu_{0z})\Delta t$$

$$\frac{P_0(t+\Delta t) - P_0(t)}{\Delta t} = P_z(t)\,\lambda_{0z} - P_0(t)\mu_{0z}$$

Ако $\Delta t \to 0$, добиваме:

$$\lim_{\Delta t\to 0}\frac{P_0(t+\Delta t) - P_0(t)}{\Delta t} = \lim_{\Delta t\to 0}P_z(t)\,\lambda_{0z} - P_0(t)\mu_{0z}) \qquad (7.30)$$

односно

$$\frac{dP_0(t)}{dt} = P_z(t)\,\lambda_{0z} - P_0(t)\mu_{0z}$$

при што со примена на Лапласова трансформација и замена во (7.30), следува:

$$sL[P_0(t)] - P_0(0) - L\lambda_{0z}P_z(t) + L\mu_{0z}P_0(t) = 0$$
$$sL[P_0(t)] - L\lambda_{0z}P_z(t) + L\mu_{0z}P_0(t) = P_0(0)$$
$$-L\lambda_{0z}P_z(t) + L(s+\mu_{0z})[P_0(t)] = P_0(0) \qquad (7.31)$$

Доколку се претпостави дека на почетокот немало настани, односно сервисот бил активен и се наоѓал во состојба 1, следува дека $P_1(0) = 1$, $P_z(0) = 0$ и $P_0(0) = 0$, тогаш со замена во (7.27), (7.29) и (7.31) имаме:

$$\begin{aligned}(\mathrm{s}+\lambda_{1z})\mathrm{L}[\mathrm{P}_1(t)] \quad & -\mu_{z1}\mathrm{L}[\mathrm{P}_z(t)] & = 1\\ -\lambda_{1\mathrm{z}}\mathrm{L}[\mathrm{P}_1(t)] + (\mathrm{s}+\mu_{\mathrm{z}1}+\lambda_{\mathrm{z}0})\mathrm{L}[\mathrm{P}_z(\mathrm{t})] \quad & -\mu_{\mathrm{z}0}\,\mathrm{L}[\mathrm{P}_0(\mathrm{t})] & = 0\\ -\lambda_{0\mathrm{z}}\mathrm{L}[\mathrm{P}_\mathrm{z}(t)] + (\mathrm{s}+\mu_{0\mathrm{z}})\mathrm{L}[\mathrm{P}_0(\mathrm{t})] & & = 0\end{aligned}$$

За да се продолжи со понатамошно решавање на системот равенките за веројатностите во состојбите на сервисот 1, z и 0, потребно е да се воведат детерминанти, за равенките (7.27), (7.29) и (7.31).

Со користење на Крамеровите правила и одбележувајќи ја со Δs детерминантата на системот, а со Δ_1, Δ_z и Δ_0 детерминантите во кои е извршена замена во првата, втората и третата колона со слободни коефициенти, се добиваат соодветни решенија во форма на Лапласова трансформација.

$$\Delta_s = \begin{vmatrix} \mathrm{s}+\lambda_{1z} & -\mu_{z1} & 0 \\ -\lambda_{1\mathrm{z}} & \mathrm{s}+\mu_{\mathrm{z}1}+\lambda_{\mathrm{z}0} & -\mu_{\mathrm{z}0} \\ 0 & -\lambda_{0\mathrm{z}} & \mathrm{s}+\mu_{0\mathrm{z}} \end{vmatrix} \qquad \Delta_1 = \begin{vmatrix} 1 & -\mu_{z1} & 0 \\ 0 & \mathrm{s}+\mu_{\mathrm{z}1}+\lambda_{\mathrm{z}0} & -\mu_{\mathrm{z}0} \\ 0 & -\lambda_{0\mathrm{z}} & \mathrm{s}+\mu_{0\mathrm{z}} \end{vmatrix}$$

$$\Delta_z = \begin{vmatrix} \mathrm{s}+\lambda_{1z} & 1 & 0 \\ -\lambda_{1\mathrm{z}} & 0 & -\mu_{\mathrm{z}0} \\ 0 & 0 & \mathrm{s}+\mu_{0\mathrm{z}} \end{vmatrix} \qquad \Delta_0 = \begin{vmatrix} \mathrm{s}+\lambda_{1z} & -\mu_{z1} & 1 \\ -\lambda_{1\mathrm{z}} & \mathrm{s}+\mu_{\mathrm{z}1}+\lambda_{\mathrm{z}0} & 0 \\ 0 & -\lambda_{0\mathrm{z}} & 0 \end{vmatrix}$$

$$\begin{aligned}\mathrm{L}[\mathrm{P}_1(t)] &= \frac{\Delta_1}{\Delta_s}\\ &= \frac{(\mathrm{s}+\mu_{\mathrm{z}1}+\lambda_{\mathrm{z}0})(\mathrm{s}+\mu_{0\mathrm{z}})-\mu_{\mathrm{z}0}\lambda_{0\mathrm{z}}}{(\mathrm{s}+\lambda_{1z})(\mathrm{s}+\mu_{\mathrm{z}1}+\lambda_{\mathrm{z}0})(\mathrm{s}+\mu_{0\mathrm{z}})-\mu_{\mathrm{z}0}\lambda_{0\mathrm{z}}(\mathrm{s}+\lambda_{1z})-\lambda_{1\mathrm{z}}\mu_{z1}(\mathrm{s}+\mu_{0\mathrm{z}})}\\ &= \frac{\mathrm{s}^2+(\mu_{\mathrm{z}1}+\lambda_{\mathrm{z}0}+\mu_{\mathrm{z}0})\mathrm{s}+\mu_{\mathrm{z}0}\mu_{\mathrm{z}1}}{\mathrm{s}[(\mathrm{s}^2+s(\lambda_{1z}+\mu_{\mathrm{z}1}+\mu_{0\mathrm{z}}+\lambda_{\mathrm{z}0})+\mu_{\mathrm{z}0}\mu_{z1}+\lambda_{1z}\mu_{0\mathrm{z}}+\lambda_{1\mathrm{z}}\lambda_{0\mathrm{z}}]}\end{aligned} \tag{7.32}$$

$$\begin{aligned}\mathrm{L}[\mathrm{P}_z(t)] &= \frac{\Delta_z}{\Delta_s}\\ &= \frac{\lambda_{1\mathrm{z}}(\mathrm{s}+\mu_{0\mathrm{z}})}{(\mathrm{s}+\lambda_{1z})(\mathrm{s}+\mu_{\mathrm{z}1}+\lambda_{\mathrm{z}0})(\mathrm{s}+\mu_{0\mathrm{z}})-\mu_{\mathrm{z}0}\lambda_{0\mathrm{z}}(\mathrm{s}+\lambda_{1z})-\lambda_{1\mathrm{z}}\mu_{z1}(\mathrm{s}+\mu_{0\mathrm{z}})}\\ &= \frac{\lambda_{1\mathrm{z}}(\mathrm{s}+\mu_{0\mathrm{z}})}{\mathrm{s}[(\mathrm{s}^2+S(\lambda_{1z}+\mu_{\mathrm{z}1}+\mu_{0\mathrm{z}}+\lambda_{\mathrm{z}0})+\mu_{\mathrm{z}0}\mu_{z1}+\lambda_{1z}\mu_{0\mathrm{z}}+\lambda_{1\mathrm{z}}\lambda_{0\mathrm{z}}]}\end{aligned} \tag{7.33}$$

$$\begin{aligned}\mathrm{L}[\mathrm{P}_0(t)] &= \frac{\Delta_0}{\Delta_s}\\ &= \frac{\lambda_{1\mathrm{z}}\lambda_{0\mathrm{z}}}{(\mathrm{s}+\lambda_{1z})(\mathrm{s}+\mu_{\mathrm{z}1}+\lambda_{\mathrm{z}0})(\mathrm{s}+\mu_{0\mathrm{z}})-\mu_{\mathrm{z}0}\lambda_{0\mathrm{z}}(\mathrm{s}+\lambda_{1z})-\lambda_{1\mathrm{z}}\mu_{z1}(\mathrm{s}+\mu_{0\mathrm{z}})}\end{aligned} \tag{7.34}$$

$$= \frac{\lambda_{1z}\lambda_{0z}}{s[(s^2 + s(\lambda_{1z} + \mu_{z1} + \mu_{0z} + \lambda_{z0}) + \mu_{z0}\mu_{z1} + \lambda_{1z}\mu_{0z} + \lambda_{1z}\lambda_{0z}]}$$

Трите равенки (7.32), (7.33) и (7.34) имаат ист именител, при што доколку се употреби $r_{1,2}$ како решение на квадратна равенка, следува:

$$s^2 + s(\lambda_{1z} + \mu_{z1} + \mu_{0z} + \lambda_{z0}) + \mu_{z0}\mu_{z1} + \lambda_{1z}\mu_{0z} + \lambda_{1z}\lambda_{0z} = 0$$

$$r_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$a = 1$$

$$b = \lambda_{1z} + \mu_{z1} + \mu_{0z} + \lambda_{z0}$$

$$c = \mu_{z0}\mu_{z1} + \lambda_{1z}\mu_{0z} + \lambda_{1z}\lambda_{0z}$$

$$r_{1,2} = \frac{-(\lambda_{1z} + \mu_{z1} + \mu_{0z} + \lambda_{z0}) \pm \sqrt{(\lambda_{1z} + \mu_{z1} + \mu_{0z} + \lambda_{z0})^2 - 4(\mu_{z0}\mu_{z1} + \lambda_{1z}\mu_{0z} + \lambda_{1z}\lambda_{0z})}}{2} \quad (7.35)$$

Доколку решенијата $r_{1,2}$ за квадратната равенка се заменат во форма на Лапласова трансформација со разложување на коефициенти, за (7.32) , следи:

$$L[P_1(t) = \frac{s^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})s + \mu_{z0}\mu_{z1}}{s(s - r_1)(s - r_2)} = \frac{K_1}{s} + \frac{K_2}{(s - r_1)} + \frac{K_3}{(s - r_2)}$$

$$K_1 = sL[P_1(t)|_{s=0} = \frac{s^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})s + \mu_{z0}\mu_{z1}}{(s - r_1)(s - r_2)} \Rightarrow \mathbf{K_1} = \frac{\mu_{z0}\mu_{z1}}{r_2 r_1}$$

$$K_2 = (s - r_1)L[P_1(t)|_{s=r_1} = \frac{s^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})s + \mu_{z0}\mu_{z1}}{s(s - r_2)} \Rightarrow$$

$$\mathbf{K_2} = \frac{{r_1}^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_1 + \mu_{z0}\mu_{z1}}{r_1(r_1 - r_2)}$$

$$K_3 = (s - r_2)L[P_1(t)|_{S=r_2} = \frac{s^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})s + \mu_{z0}\mu_{z1}}{s(s - r_1)} \Rightarrow$$

$$\mathbf{K_3} = \frac{{r_2}^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_2 + \mu_{z0}\mu_{z1}}{r_2(r_2 - r_1)}$$

Со замена на вредностите за $\mathbf{K_1}$, K_2и K_3 во $L[P_1(t)$:

$$L[P_1(t)] = \frac{\frac{\mu_{z0}\mu_{z1}}{r_2 r_1}}{s} + \frac{\frac{r_1^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_1 + \mu_{z0}\mu_{z1}}{r_1(r_1 - r_2)}}{(s - r_1)} + \\ + \frac{\frac{r_2^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_2 + \mu_{z0}\mu_{z1}}{r_2(r_2 - r_1)}}{(s - r_2)} \tag{7.36}$$

Доколку решенијата $r_{1,2}$ за квадратната равенка се заменат во форма на Лапласова трансформација со разложување на коефициенти, за (7.33) , следи:

$$L[P_z(t)] = \frac{\lambda_{1z}(s + \mu_{0z})}{s(s - r_1)(s - r_2)} = \frac{K_1}{s} + \frac{K_2}{(s - r_1)} + \frac{K_3}{(s - r_2)}$$

$$K_1 = sl[P_z(t)|_{s=0} = \frac{\lambda_{1z}(s + \mu_{0z})}{(s - r_1)(s - r_2)} \qquad \Rightarrow K_1 = \frac{\mu_{z0}\lambda_{1z}}{r_2 r_1}$$

$$K_2 = (s - r_1)L[P_z(t)|_{s=r_1} = \frac{\lambda_{1z}(s+\mu_{0z})}{s(s-r_2)} \qquad \Rightarrow K_2 = \frac{\lambda_{1z}(r_1 + \mu_{0z})}{r_1(r_1 - r_2)}$$

$$K_3 = (s - r_2)L[P_z(t)|_{s=r_2} = \frac{\lambda_{1z}(s + \mu_{0z})}{s(s - r_1)} \qquad \Rightarrow K_3 = \frac{\lambda_{1z}(r_2 + \mu_{0z})}{r_2(r_2 - r_1)}$$

Со замена на вредностите за K_1 , K_2и K_3 во (7.33):

$$L[P_z(t) = \frac{\frac{\mu_{z0}\lambda_{1z}}{r_2 r_1}}{s} + \frac{\frac{\lambda_{1z}(r_1 + \mu_{0z})}{r_1(r_1 - r_2)}}{(s - r_1)} + \frac{\frac{\lambda_{1z}(r_2 + \mu_{0z})}{r_2(r_2 - r_1)}}{(s - r_2)} \tag{7.37}$$

Доколку решенијата $r_{1,2}$ за квадратната равенка се заменат во форма на Лапласова трансформација со разложување на коефициенти, за (7.34) , следи:

$$L[P_0(t) = \frac{\lambda_{1z}\lambda_{0z}}{s(s - r_1)(s - r_2)} = \frac{K_1}{s} + \frac{K_2}{(s - r_1)} + \frac{K_3}{(s - r_2)}$$

$$K_1 = sL[P_0(t)|_{s=0} = \frac{\lambda_{1z}\lambda_{0z}}{(s - r_1)(s - r_2)} \qquad \Rightarrow K_1 = \frac{\lambda_{1z}\lambda_{0z}}{r_2 r_1}$$

$$K_2 = (s - r_1)L[P_0(t)|_{s=r_1} = \frac{\lambda_{1z}\lambda_{0z}}{s(s - r_2)} \qquad \Rightarrow K_2 = \frac{\lambda_{1z}\lambda_{0z}}{r_1(r_1 - r_2)}$$

$$K_3 = (S - r_2)L[P_0(t)|_{s=r_2} = \frac{\lambda_{1z}\lambda_{0z}}{s(s - r_1)} \qquad \Rightarrow K_3 = \frac{\lambda_{1z}\lambda_{0z}}{r_2(r_2 - r_1)}$$

Со замена на вредностите за K_1 , K_2 и K_3 во (7.34):

$$L[P_0(t)] = \frac{\frac{\lambda_{1z}\lambda_{0z}}{r_2 r_1}}{s} + \frac{\frac{\lambda_{1z}\lambda_{0z}}{r_1(r_1 - r_2)}}{(s - r_1)} + \frac{\frac{\lambda_{1z}\lambda_{0z}}{r_2(r_2 - r_1)}}{(s - r_2)} \tag{7.38}$$

Функцијата за распожливост на сервисот претставена со помош на функциите за веројатност на состојбата на сервисот, претставени со Лапласовата трансформација е:

$$L[A(t)] = L[P_1(t)] + L[P_z(t)] \tag{7.39}$$

За понатамошно решавање на функцијата за распожливост на сервисот претставена со Лапласова трансформација, потребно е да се земат во предвид следните идентитети:

$$r_1 + r_2 = -(\lambda_{1z} + \mu_{z1} + \mu_{0z} + \lambda_{z0}) \tag{7.40}$$

$$r_1 r_2 = \mu_{z0}\mu_{z1} + \lambda_{1z}\mu_{0z} + \lambda_{1z}\lambda_{0z} \tag{7.41}$$

$$L[A(t)] = \frac{\frac{\mu_{z0}\mu_{z1}}{r_2 r_1}}{s} + \frac{\frac{r_1^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_1 + \mu_{z0}\mu_{z1}}{r_1(r_1 - r_2)}}{(s - r_1)} +$$

$$+ \frac{\frac{r_2^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_2 + \mu_{z0}\mu_{z1}}{r_2(r_2 - r_1)}}{(s - r_2)} + \frac{\frac{\mu_{z0}\lambda_{1z}}{r_2 r_1}}{s} + \frac{\frac{\lambda_{1z}(r_1 + \mu_{0z})}{r_1(r_1 - r_2)}}{(s - r_1)} + \frac{\frac{\lambda_{1z}(r_2 + \mu_{0z})}{r_2(r_2 - r_1)}}{(s - r_2)} =$$

$$= \frac{\frac{\mu_{z0}\mu_{z1} + \mu_{z0}\lambda_{1z}}{r_2 r_1}}{s} + \frac{\frac{r_1^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_1 + \mu_{z0}\mu_{z1} + \lambda_{1z}(r_1 + \mu_{0z})}{r_1(r_1 - r_2)}}{(s - r_1)} +$$

$$+ \frac{\frac{r_2^2 + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_2 + \mu_{z0}\mu_{z1} + \lambda_{1z}(r_2 + \mu_{0z})}{r_2(r_2 - r_1)}}{(s - r_2)}$$

$$L[A(t)] = \frac{\frac{\mu_{z0}\mu_{z1} + \mu_{z0}\lambda_{1z}}{r_2 r_1}}{s} + \frac{\frac{r_1^{\,2} + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_1 + \mu_{z0}\mu_{z1} + \lambda_{1z}(r_1 + \mu_{0z})}{r_1(r_1 - r_2)}}{(s - r_1)} + \frac{\frac{r_2^{\,2} + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_2 + \mu_{z0}\mu_{z1} + \lambda_{1z}(r_2 + \mu_{0z})}{r_2(r_2 - r_1)}}{(s - r_2)} \quad (7.42)$$

Со наоѓање на инверзна Лапалсова трансформација, се добиваат следните равенки за функцијата за распожливост на сервисот A(t):

*) од таблицата за Лапласова трансформација се добиваат следните замени:

$$L[1] = \frac{1}{s} \qquad L[e^{bt}] = \frac{1}{s - b} \qquad L[e^{-bt}] = \frac{1}{s + b}$$

Функцијата за расположливост на сервисот, како функција од времето се добива:

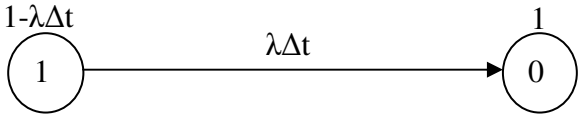
$$A(t) = \frac{\mu_{z0}\mu_{z1} + \mu_{z0}\lambda_{1z}}{r_2 r_1} + \frac{r_1^{\,2} + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_1 + \mu_{z0}\mu_{z1} + \lambda_{1z}(r_1 + \mu_{0z})}{r_1(r_1 - r_2)} e^{r_1 t} + \frac{r_2^{\,2} + (\mu_{z1} + \lambda_{z0} + \mu_{z0})r_2 + \mu_{z0}\mu_{z1} + \lambda_{1z}(r_2 + \mu_{0z})}{r_2(r_2 - r_1)} e^{r_2 t} \quad (7.43)$$

7.4 Веродостојност на сервисите во сервисно ориентиран информациски систем

Функцијата на веродостојноста на сервисот претставува веројатност за работа на сервисот во временски интервал од 0 до t. При тоа, за интензитетот за недостапност на сервисот, исто така ќе се земе константна вредност $\lambda = const$.

Употребата на Марковите модели е најпогодна за испитување на веродостојноста на сервисот. Состојбите во кои може да се најде сервисот се 1 и 0. Во состојба 1 сервисот е активен, додека во состојба 0 истиот не е активен. Ние ќе испитуваме веродостојност на сервисот, кога сервисот работи во временски интервал од 0 до t.

Графичкиот модел за веродостојноста на сервисот со употреба на Маркови модели (Слика 37), ќе биде:



Слика 37. Дијаграм на транзиција (преоѓање) на состојбите

Врз основа на графичкиот модел, ќе важи и следниот табеларен приказ (Табела 6):

Табела 6. Матрица на веројатност за транизиција на сервисот

Почетна состојба на сервисот	Крајна состојба (t+Δt)	
	1	0
1	1-λΔt	λΔt
0	0	1

Ова е специјален случај на сервисот во Случај I, кога μ=0. Оттука со замена (на μ=0) во (7.26) се добива:

$$P_0(t) = 1 - e^{-\lambda t} \tag{7.44}$$

Така да врз основа на наведеното, можеме да заклучиме дека веродостојност на сервисот ќе коренспондира на состојбата 1 на сервисот, во време t, односно сервисот е активен или достапен за користење.

$$R(t) = e^{-\lambda t} \tag{7.45}$$

За разлика од достапноста на сервисот во состојба 1, сервисот е недостапен кога тој се наоѓа во состојба 0, при што следува дека сервисот е неверодостоен за користење во временски момент t со веројатност $P_0(t)$.

$$Q(t) = 1 - e^{-\lambda t} \tag{7.46}$$

7.4.1 Пример 2

Првата состојба на сервисот при одреден упит или повеќе упити од поголем број на клиенти во одреден момент t, ќе коренспондира на претпоставката дека сервисот е достапен или активен за користење од страна на корисниците. Таа состојба на сервисот ќе ја означиме со 1.

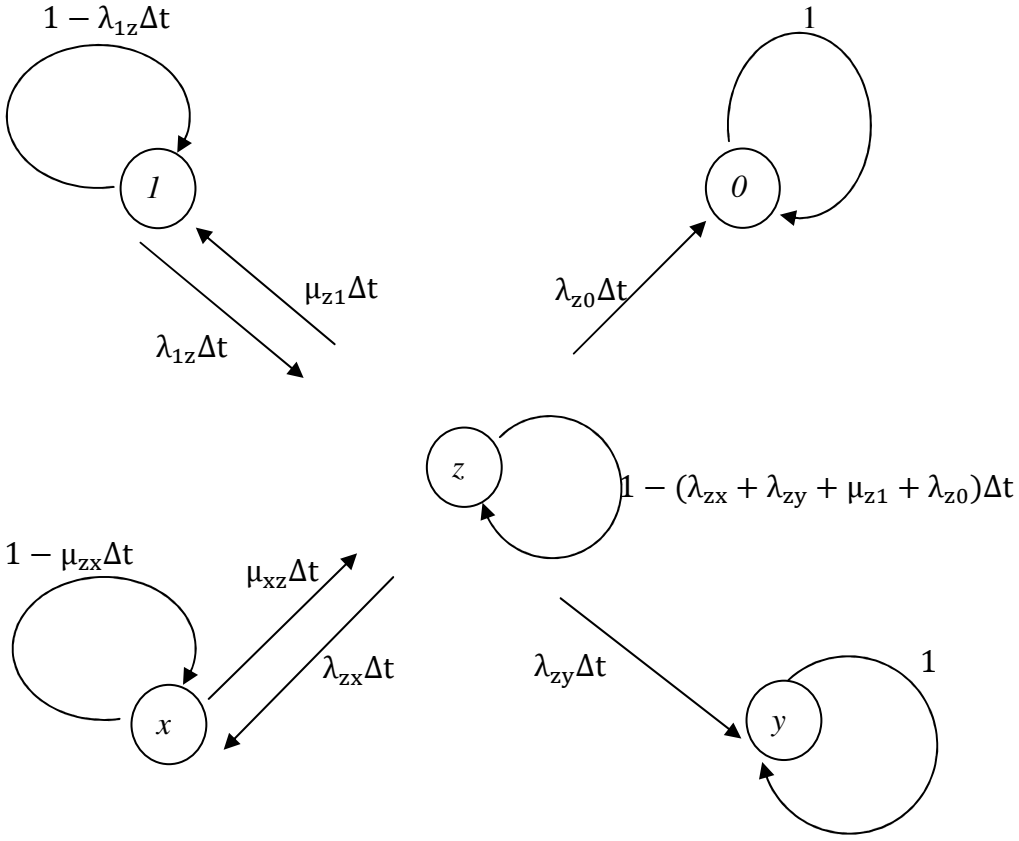
Доколку сервисот во одреден момент Δt премине во неактивна состојба, односно е недостапен за корисниците, тогаш тој преминува во неактивна состојба, која ќе ја означуваме со j.

Двата случаи кои се однесуваат за состојбите на сервисот кога тој се наоѓа во состојба 1 и j се разработени во претходната секција.

Состојбите кои ќе ги презентираме се однесуваат на состојби во кои може да се најде сервисот во временски момент кога веројатноста за добивање на одговор од сервисот е еднаква со веројатноста кога се очекува и недобивање на одговор. Така што, ќе воведеме состојба z, која ќе се однесува на состојба на сервисот кога тој ќе го процесира упит од клиентите. Како резултат на преоѓање на системот во оваа состојба, тој понатаму може да продолжи во двете состојби со иста веројатност за добивање или недобивање на

одговор од сервисот. Доколку имаме одоговор од сервисот, тогаш тој ќе премине во состојба која ќе ја дефинираме со x. Доколку сервисот премине од состојбата z во состојба каде постои веројатноста за недобивање на одговор, тогаш таа состојба во која се наоѓа сервисот ќе ја дефинираме како y.

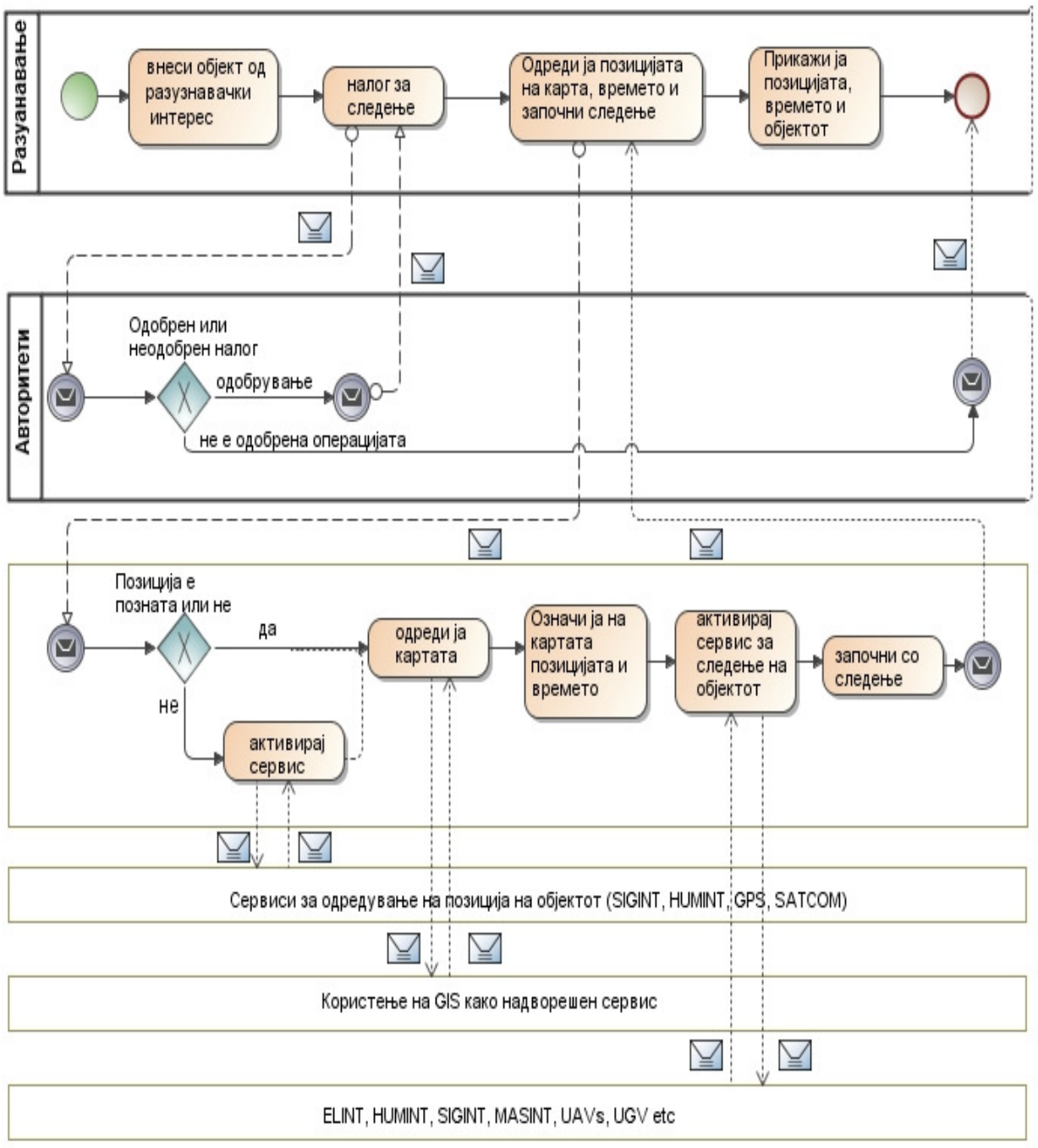
Врз основа на претходно наведеното, состојбите низ кои сервисот може да се движи, односно транзицијата на состојбите (Слика 38), ќе се претстави со следниот дијаграм:



Слика 38. Дијаграм на транзиција (преоѓање) на состојбите

Овој случај е специјален случај на системот од Пример 1 (даден на Слика 36), кој се добива за $\mu_{zo}=0$. Оттука, со замена на $\mu_{zo}=0$ во (7.43) за функцијата на расположливост на сервисот се добива:

$$A(t)=\frac{r_1+\mu_{z1}+\lambda_{z0}+\lambda_{1z}}{(r_1-r_2)}e^{r_1 t}-\frac{\mu_{z1}+\lambda_{z0}+r_2+\lambda_{1z}}{(r_1-r_2)}e^{r_2 t} \qquad (7.47)$$



Слика 39. Бизнис процес за следење на објект од разузнавачки интерес

Според прикажаниот бизнис процес (Слика 39) употребен за да се демонстрира функционалноста на информацискиот систем за разузнавање, пред да се започне одредена разузнавачка операција потребно е да се добие налог во форма на решение, наредба или некоја друга форма, согласно законската процедура, одобрен од страна на авторитетите. Налогот начелно би требало да содржи следните елементи: објект на разузнавачки интерес, која разузнавачка операција ќе се извршува, време од кога да започне

операцијата и истата кога да заврши и други пропратни елементи кои имаат за цел поуспешно спроведување на операцијата.

Доколку разузнавачката операција не е одобрена од авторитетите, истата веднаш завршува.

Доколку разузнавачката операција е одобрена за извршување врз објектот на разузнавачки интерес, односно е одобрен налогот, тогаш бизнис процесот продолжува со одредување на позицијата и времето. Исто така треба да се напомене дека во нашиот случај е селектирано следење на објектот од разузнавачки интерес како разузнавачка операција.

За да може да се одреди позицијата на одреден објект потребно е да се активираат сервиси кои може да се компоненти на информацискиот систем за разузнавање или пак истите да се користат од надворешен сервис провајдер.

Сервисот „HUMINT (Human Intelligence)“ или човечкото разузнавање е најстариот и најпровереният начин на собирање на податоци и разузнавачки информации. Методологијата односно начинот на кој се доаѓа до потребните податоци може да биде преку отворено, прикриено и тајно собирање на податоците. Собраните податоци преку средства за комуникација се дистрибуираат и се зачувуваат во бази на податоци од информацискиот систем за разузнавање.

Сервисот „SIGINT (Signals Intelligence)“ или сигнално разузнавање претставува термин за разузнавање кое се извршува преку гониометрирање на сигналите од средствата за комуникација. Може да се реализира од разни оддалечени локации на копно, со употреба на авиони или сателити.

Сервисот „IMINT (Imagery Intelligence)“ или разузнавање со употреба на слики, се извршува со помош на визуелни фотографии, инфрацрвени сензори, ласери, електрооптички уреди и радарски сензори (со кои се добиваат фотографии со помош на сателит).

Сервисот „MASINT (Measurement and Signatures Intelligence)“ или разузнавање преку мерење и означување (лоцирање), е разузнавање кое лоцира , идентификува или опишува специфични карактеристики на објектите. За добивање на овие информации се користат голем број дисциплини меѓу кои и нуклеарни, оптички, радиофреквентна, акустика, сеизмика и други природни науки.

Несекогаш за одредување на позицијата на објектот мора да користат наведените сервиси. Во зависност од технолошкиот развој можно е користење и на други сервиси чии придобивки ќе може да се користат во иднина.

Позицијата на објектот потребно е да се означи на дигитална карта, а тоа е овозможено со користење на „Geographic Information System (GIS)“. Користењето на гео-информацискиот систем од информацискиот систем за разузнавање е компонента како сервис од надворешен сервис провајдер. Со користењето на гео-информацискиот систем за одредување на позицијата на објектот и нејзино означување на дигитална карта се овозможува софистицирано извршување на разузнавачката операција. Со ова се овозможува креирање на неколку сценарија на можните рути каде што би можел да се движи објектот.

Сервисите за следење на објектот се активираат по означувањето на позицијата на карта. Во зависност од тоа кој сервис ќе се користи за следење ќе зависи и начинот на следење. На пример, доколку се користи беспилотно летало како сервис за извршување на разузнавачката операција, тогаш е потребно остварување на конекција со гео-

информацискиот систем од каде ќе користат координатите на позицијата на објектот. А како второ, беспилотното летало има „payload“, кој има видео камери со висока резолуција кои се користат за извршување на разузнавачки операции, при што е возможно и дејствување по објектот бидејќи „payload“-от може да биде вооружен, во зависност од типот на беспилотно летало.

Карактеристично за сите наведени сервиси е веројатноста за нивната употреба односно расположливоста во одреден временски момент, при извршување на разузнавачката операција. Со цел за што подобра презентација, ќе употребиме зони (Табела 8) кои ќе означуваат веројатноста за состојбата на сервисот.

Табела 8. Расположливост на сервисот со соодветни зони на употреба

Расположливост на сервисот	Зони
сервисот сигурно се употребува	
сервисот можно е да се употреби	
сервисот не може да се употреби	

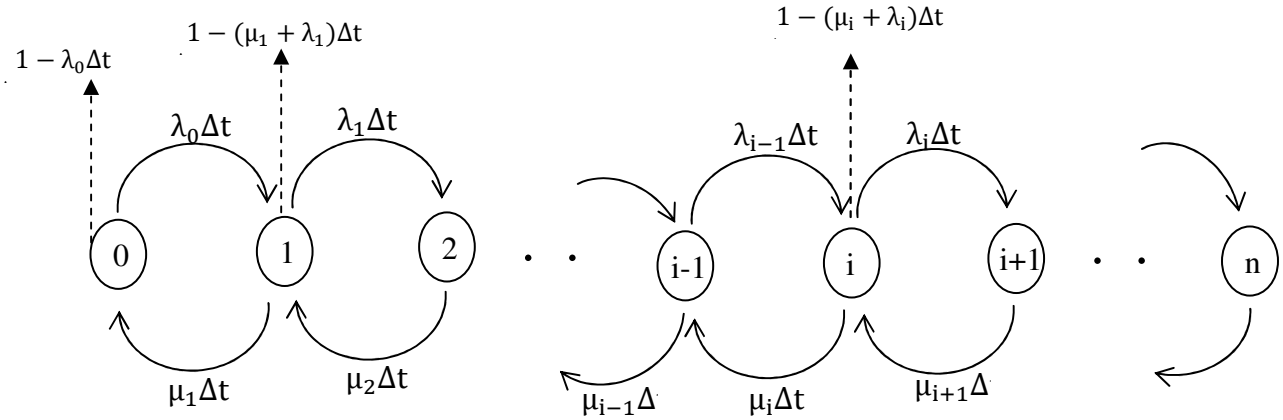
Врз основа на веројатноста за расположливост на сервисите ќе може да одредиме кои од наведените сервиси се најсоодветни за користење во одреден временски момент, за да се изврши одредена разузнавачката операција.

7.5 Пресметување на расположливост на сервисно ориентиран информациски систем

Разгледуваме сервисно ориентиран систем составен од N сервиси. При тоа, секој од сервисите може да биде во активна состојба, кога е расположлив или во неактивна состојба, кога не е расположлив за користење.

Состојбата на системот е определена со бројот на активни сервиси. Тогаш системот може да се опише со Маркова верига која определува број на активните сервиси. Вака креираната верига е конечна и може да се прими вредност од множеството E={0,1,2,…, n}. Кога веригата ќе се најде во состојба i, тогаш се активни i сервиси. Интензитетот на активност за расположливост на уште еден сервис се зголемува со λ_i. Интензитетот на неактивност односно намалување на расположливоста на сервисите во сервисно

ориентираниот информациски систем е μ_i. Врз основа на претходно наведеното може да се креира дијаграм на состојби на Маркова верига за сервисно ориентиран информациски систем (Слика 40).



Слика 40. Дијаграм на состојбите на Маркова верига за сервисно ориентиран информациски систем

Понатаму потребно е да се состават и определат веројатностите на состојбите $P_i(t)$, за i=0,1,...,n

*) за $P_0(t)$, кога сервисот се наоѓа во состојба 0,

$$P_0(t+\Delta t) = (1-\lambda_0\Delta t)P_0(t) + P_1(t)\mu_1\Delta t$$

$$P_0(t+\Delta t) - P_0(t) = (\mu_1 P_1(t) - \lambda_0 P_0(t))\Delta t$$

$$\frac{P_0(t+\Delta t) - P_0(t)}{\Delta t} = \mu_1 P_1(t) - \lambda_0 P_0(t))$$

Ако $\Delta t \to 0$, добиваме :

$$\lim_{\Delta t\to 0} \frac{P_0(t+\Delta t) - P_0(t)}{\Delta t} = \lim_{\Delta t\to 0} (\mu_1 P_1(t) - \lambda_0 P_0(t)) \qquad (7.48)$$

односно

$$\frac{dP_0(t)}{dt} = \mu_1 P_1(t) - \lambda_0 P_0(t)$$

*) за $P_i(t)$, кога сервисот се наоѓа во состојба i, i=1,2,...,n-1, се добива:

$$P_i(t+\Delta t) = P_{i-1}(t)\,\lambda_{i-1}\Delta t + P_i(t)\big(1 - (\mu_i + \lambda_i)\Delta t\big) + P_{i+1}(t)\mu_{i+1}\Delta t$$

$$P_i(t+\Delta t) - P_i(t) = P_{i-1}(t)\,\lambda_{i-1}\Delta t - P_i(t)(\mu_i + \lambda_i)\Delta t + P_{i+1}(t)\mu_{i+1}\Delta t$$

$$P_i(t+\Delta t) - P_i(t) = (P_{i-1}(t)\,\lambda_{i-1} - P_i(t)(\mu_i + \lambda_i) + P_0(t)\mu_{i+1})\Delta t$$

$$\frac{P_i(t+\Delta t) - P_i(t)}{\Delta t} = P_{i-1}(t)\,\lambda_{i-1} - P_i(t)(\mu_i + \lambda_i) + P_{i+1}(t)\mu_{i+1}$$

Ако $\Delta t \to 0$, се добива:

$$\lim_{\Delta t\to 0}\frac{\mathrm{P}_i\,(t+\Delta t)-\mathrm{P}_i\,(t)}{\Delta t}=\lim_{\Delta t\to 0}(\mathrm{P}_{\mathrm{i}-1}\,(t)\,\lambda_{\mathrm{i}-1}-\mathrm{P}_i\,(t)\big(\mu_{\mathrm{i}}+\lambda_{\mathrm{i}}\big)+\mathrm{P}_{i+1}\,(t)\mu_{i+1}) \quad (7.49)$$

односно

$$\frac{\mathrm{dP_i\,(t)}}{\mathrm{dt}}=(\mathrm{P}_{\mathrm{i}-1}\,(t)\,\lambda_{\mathrm{i}-1}-\mathrm{P}_i\,(t)\big(\mu_{\mathrm{i}}+\lambda_{\mathrm{i}}\big)+\mathrm{P}_{i+1}(t)\mu_{i+1})$$

*) за $\mathrm{P}_n(t)$, кога сервисот се наоѓа во состојба n, се добива:

$$\mathrm{P}_n(t+\Delta t)=\mathrm{P}_{\mathrm{n}-1}(t)\,\lambda_{\mathrm{n}-1}\Delta t+\mathrm{P}_n\,(t)\big(1-\mu_{\mathrm{n}}\Delta\mathrm{t}\big)$$
$$\mathrm{P}_n(t+\Delta t)-\mathrm{P}_n\,(t)=\mathrm{P}_{\mathrm{n}-1}(t)\,\lambda_{\mathrm{n}-1}\Delta t+\mu_{\mathrm{n}}\mathrm{P}_n\,(t)\Delta\mathrm{t}$$
$$\mathrm{P}_n(t+\Delta t)-\mathrm{P}_n\,(t)=(\mathrm{P}_{\mathrm{n}-1}(t)\,\lambda_{\mathrm{n}-1}+\mu_{\mathrm{n}}\mathrm{P}_n\,(t))\Delta\mathrm{t}$$

$$\frac{\mathrm{P}_n(t+\Delta t)-\mathrm{P}_n\,(t)}{\Delta t}=\mathrm{P}_{\mathrm{n}-1}(t)\,\lambda_{\mathrm{n}-1}+\mu_{\mathrm{n}}\mathrm{P}_n\,(t)$$

Ако $\Delta t\to 0$, се добива:

$$\lim_{\Delta t\to 0}\frac{\mathrm{P}_n(t+\Delta t)-\mathrm{P}_n\,(t)}{\Delta t}=\lim_{\Delta t\to 0}(\mathrm{P}_{\mathrm{n}-1}(t)\,\lambda_{\mathrm{n}-1}+\mu_{\mathrm{n}}\mathrm{P}_n\,(t)) \quad (7.50)$$

односно

$$\frac{\mathrm{dP_n\,(t)}}{\mathrm{dt}}=\mathrm{P}_{\mathrm{n}-1}(t)\,\lambda_{\mathrm{n}-1}+\mu_{\mathrm{n}}\mathrm{P}_n\,(t)$$

Наша цел е определување на веројатностите на состојбите $\mathrm{P_i(t)}$, i=0,1,...,n. Но, решавањето на асистемот диференцијални равенки, составен од равенките (7.48), (7.49) и (7.50) не е едноставна работа и бара посложени математички механизми. За да ја упростиме работата, ќе претпоставиме дека системот може да се најде во стационарен режим на работа, т.е. постои негова стационарана распределба. За да биде постигнато тоа, потребно е да важат равенствата:

$$\lim_{t\to\infty}\mathrm{P_i(t)}=\mathrm{p_i^*}\ ,\ \mathrm{i}=0,1,\dots,\mathrm{n.},$$

Векторот на веројатности $(\mathrm{p_0^*},\mathrm{p_1^*},\cdots,\mathrm{p_n^*})$, ако постои, се нарекува вектор на стационарни веројатности. Ако веригата дојде до стационарна распределба, таа останува во неа, без оглед која била почетната распределба, Во тој случај,

$$\lim_{t\to\infty}\frac{\mathrm{dP_i\,(t)}}{\mathrm{dt}}=0$$

На овој начин горните диференцијални равенки може да се трансформираат во едноставни линеарни равенки за определување на стационарните веројатности:

$$0=\ \mu_1\mathrm{p_1^*}\ -\lambda_0\mathrm{p_0^*} \quad (7.51)$$

$$0=\ \lambda_{\mathrm{i}-1}\mathrm{p_{i-1}^*}+\big(\mu_{\mathrm{i}}+\lambda_{\mathrm{i}}\big)\mathrm{p_i^*}\ +\mu_{i+1}\mathrm{p_{i+1}^*}$$
$$0=\lambda_{\mathrm{n}-1}\mathrm{p_{n-1}^*}+\mu_{\mathrm{n}}\mathrm{p_n^*} \quad (7.52)$$

Наведениот систем на равенки може да се решава рекурзивно, заменувајќи ги решенијата од една во друга равенка, последователно, односно решението од првата равенка се заменува во втората равенка, од втората во третата итн.

Со решавање на равенките по p_i^* , се добива дека

$$p_i^* = \frac{\lambda_{i-1}\lambda_{i-2} \dots \lambda_0}{\mu_i \mu_{i-1} \cdots \mu_1} p_0^* , i = 1,2, \cdots, n \tag{7.53}$$

Од решавањето на рекурзивните равенки лесно се утврдува дека во веројатноста на секоја состојба во која може да се најде сервисно ориентираниот информациски систем, зависи од p_0^* .

За да се одреди вредноста на p_0^* потребно е сите стационарни веројатности на состојбите на системот да се соберат и да се изедначат со 1.

$$\sum_{i=0}^{n} p_i^* = 1 \tag{7.54}$$

За вредноста на стационараната веројатност p_0^* , следува:

$$p_0^* = \left(1 + \sum_{i=0}^{n} \frac{\lambda_{i-1}\lambda_{i-2} \dots \lambda_0}{\mu_i \mu_{i-1} \cdots \mu_1}\right)^{-1} \tag{7.55}$$

За крај да воочиме дека поради тоа што бројот на состојби е конечен, па и сумата во (7.55) е секогаш конечна, p_0^* секогаш може да се определи. Тоа значи, дека за ваквата верига, стационарана распределба сигурно ќе постои, па кога системот ќе ја достигне истата, останува во неа постојано.

7.6 Време на одзив на сервисот

Време на одзив на сервисот (*engl.*Service Response Time (SRT)) е вкупното време што поминува помеѓу последниот бајт на доставеното барање до сервисот и последниот бајт на одговорот на сервисот. За да се заврши сервисната трансакција, за некои сервиси е потребна единечна интеракција, додека за други е потребна повеќекратна интеракција. Како резултат, во случај на сервиси со единечна интеракција, „SRT“ е времето потребно за да се заврши комплетната трансакцијата, додека во случај на сервиси со повеќекратна интеракција, „SRT“ претставува време земено да се комплетира една интеракција за одредена трансакција.

$$SRT = \sum_{i=1}^{n} [SRT_1^{(i)} - SRT_2^{(i)}] \tag{7.56}$$

T_1 – време во кое веб сервисот доставува SOAP одзив
T_2 – време во кое е доставен SOAP упит до веб сервисот

За да се измери времето на одзив на сервисите, во зависност од принципите на СОА, потребно е да се има во предвид следното ([114]):

- Сервисите и сервисните клиенти се лоцирани на различни локации, најчесто на различни машини;
- Употреба на стандардниот формат за пораки, „XML“, го зголемува времето потребно за процесирање на барањето;
- Сервисите може да бидат откриени во времето на дизајн или во текот на времето со отпочнување на нивното користење или преку употреба на сервиси за откривање или со агенти;
- Сервисите кои ги подредуваат бизнис процесите може да се искористат во одговор на потребите за бизнис процесите;
- Сервисната композиција можеби би требало да биде адаптирана со додавање на дополнителни сервиси или со вметнување во адаптираните сервиси.

Основната причина за ниските перформанси на СОА вообичаено потекнуваат од овие фактори. Поради тоа е потребно креирање на метрики за времето за одзив на сервисите, при тоа земајќи ги во предвид наведените фактори.

За информацискиот систем за разузнавање потребно е да се обработи следната проблематика за времето за одзив:

- ИСР е составен од 1, …, n_{IIS} сервиси, а тоа значи дека ќе има од $t \in [1,t_n]$ времиња за одзив на сервисите од ИСР;
- ИСР ќе се поврзува со други системи базирани на сервисно ориентирана архитектура, при што ќе биде потребно да се пресмета исто така времето за одзив, при што ќе имаме 1, ..., n_{isoa} сервиси од информациските системи базирани на СОА и ќе имаме $t \in [1,t_n]$ времиња за одзив;

ГЛАВА 8

ЗАКЛУЧОК

Моделот на информациски систем за разузнавање претставен во оваа теза дава придонес во јакнење на Националната безбедност и соодветна проценка во цивилно-воените ризици преку обезбедување на информации со имплементирање на механизми за извлекување и вметнување на информации во информацискиот систем, потоа со селектирање на податоци и креирање на информации од необработени податоци, кои може да бидат употребени во креирање на разузнавачки продукти и дисиминација на известувања до авторитетите. Во докторската дисертација, тоа е направено со ИСР базиран на СОА, која ги прати петте предложени постулати кои овозможуваат флексибилен и безбедносен дизајн на ИСР.

Нивото на технолошки развој во одредени општества извршува притисок за користење на придобивките од имплементирањето на современата технологијата кои што придобивките директно зависат од нивото на развој на самото општество. Како резултат, може да се констатира дека како што бројот на информациски системи и податоци се зголемува, во исто време проблемот со интеграцијата на информациите и податоците претставува поголем предизвик. Со цел оптимално да се да се искористат селектираните системи, предложениот модел за интеграција претставува едно можно решение. Интегрирањето на информациските системи треба да се базира на претпоставката дека секој информациски систем може да е самостојна индивидуална единица која содржи сопствени податоци, но за да се користат информациите од секој систем потребно е воспоставување на високо ниво на синергија помеѓу системите со цел да се споделуваат (*engl.* sharing) информациите.

Елаборираните секции во поглавјето за интеграција на информациските системи, овозможуваат одредување на најсоодветен модел за интеграција на информациските системи, а исто така е предложено и соодветно решенение за интеграција, односно архитектура каде примачот и предавачот на пораката директно комуницираат со пораки при што се поврзани „point-to-point“ интеграцискиот модел за информациски системи.

Разработениот модел за интеграција на информациските системи е соодветен бидејќи овозможува размена на сите типови на податоци и овозможува едноставно надоградување на нови системи следејќи ги современите стандарди.

Презентиран модел на сигурносно решение за информацискиот систем за разузнавање базиран на СОА парадигимата, овозможува да се постигне сигурен тек на податоците низ информацискиот систем, без последици по сигурносните полиси како што се автентификација, интегритет, авторизација, приватност и неможност за одрекување.

Предложениот модел дозволува забележување на барањата и нарушувањето на сигурносните полиси на соодветен начин. Исто така, презентираниот модел на комплексно структурирано решение е лесен за имплементирање и ги содржи сите современи сигурносни полиси и протоколи, при што истиот не предизвикува негативни импликации врз останатите софтверски компоненти на моделот на информаци систем.

Имплементацијата на сервисно ориентираната архитектура во информационен систем за разузнавање ќе ја зголеми ефикасноста на разузнавањето. Основа за развој на одреден информационен систем е постоење на утврдена методологија и модел.

Во докторската дисертација се предложени *генерални метрики* кои ќе бидат употребени за евалуирање на сервисите во сервисно ориентиран систем и *специјални метрики* кои се однесуваат на евалуирање на сервисите во информациски систем за разузнавање базиран на СОА. Исто така, опишани се метриките и приложени се референтни вредности кои е потребно да се користат за презентирање на резултатите на соодветен начин. Една од предностите на предложените метрики е дека тие може да бидат употребени за секој сервис или сервисна композиција.

Предложениот сет на метрики не е дефинитивно сеопфатен, но претставува добра основа за дискусија и понатамошно истражување во ова поле. Наведените метрики даваат придонес во развој на спецификациите на сервисите кои треба да бидат креирани во информациските системи за разузнавање. Други аспекти за евалуација на сервисите исто така треба да бидат земени во предвид.

Во однос на проценувањето на веројатноста за достапност на сервисите и веројатноста за недостапност на сервисите, преку законот за распределба на веројатност се овозможува приказ на функционалноста на сервисите од информацискиот систем независно од времето како параметар.

Несекогаш е потребно времето да се зема во предвид, односно тоа да биде потребна информација која ќе има значајно влијание на некој настан. Информациите добиени од сервисите кога времето не е земено во предвид, финасиски е поевтино бидејќи не се прават дополнителни трошоци, а директно се користи информацијата добиена од сервисот (видео камера, беспилотно летало, воздухоплов, сателит итн.)

Атрибутите на сервисите претставуваат важна карактеристика. Преку креирање на метрики за атрибутите на сервисите се овозможува селектирање за користење на најпогодниот сервис, во однос на извршување на одредена разузнавачка операција. Одредувањето на веродостојноста, расположливоста и очекуваното време за одзив на сервисите во информацискиот систем за разузнавање е презентирано со цел да се даде приказ за функционалноста на системот преку проценување на веројатноста на сервисите во одреден временски момент. Проценувањето на наведените атрибути дава можност за организирање во однос на употреба на најсоодветните сервиси од системот, со што би се постигнала оптимизација за извршување на разузнавачката операција.

Од друга страна, креирањето на модел на систем за разузнавање, придонесува во лимитирано учество на човечкиот фактор во разузнавањето. Наведеното може да се користи во позитивна и негативна смисла.

Позитивен контекст е пред се, користење на информациите. Разузнавачките информации не секогаш се достапни согласно принципите на разузнавањето. Со информацискиот систем се постигнува споделување на информациите согласно принципите, а врз основа на нив, се донесуваат правилни одлуки.

Негативниот контекст ја истакнува можноста од пробивање во информацискиот систем и предизвикување на последици по општеството или националната безбедност на државата.

ЛИТЕРАТУРА

[1] Air Combat Command, - Version 2, CONOPS UAV, Section 6 - Communication Integration and Interoperability, http://www.fas.org/irp/doddir/usaf, US Air Force; 3 Dec 1996

[2] Anurag Goel, Enterprise Integration EAI vs. SOA vs. ESB, http://hosteddocs.ittoolbox.com/Enterprise%20Integration%20%20SOA%20vs%20EAI%20vsESB.pdf, consulted of January 2011

[3] Farzad Sanati, Jie Lu "A Methodological Framework for E-government Service Delivery Integration" Faculty of Information Technology, University of Technology, Broadway NSW. 2007

[4] Baglietto, P., M. Maresca, et al.. "Stepwise deployment methodology of a service oriented architecture for business communities." Journal: Information and Software Technology 47(6): 427-436. 2005

[5] Belanger, F. and L. D. Carter "U-government: a framework for the evolution of e-government." International Journal: Electronic Government **2**(4): 426-445. 2005

[6] Hepp, M. "Semantic Web and Semantic Web Services." IEEE INTERNET COMPUTING. 2006.

[7] Burk, R. R..: "Enabling Citizen-Centered Electronic Government 2005-2006 Action Plan"; USA, Office of E-Government and Information Technology. 2005

[8] Burstein, M. H.. "Dynamic Invocation of Semantic Web Services That Use Unfamiliar Ontologies." IEEE INTELLIGENT SYSTEMS (JULY/AUGUST). (vol. 19 no. 4) 2004

[9] Castellano, M.. "An e-Government Cooperative Framework for Government Agencies". 38th Hawaii International Conference on System Sciences. Hawaii, IEEE. 2005

[10] Arroyo, S., M.-A. Sicilia, et al.. "Choreography frameworks for business integration: Addressing heterogeneous semantics." Journal: Computers in Industry.2006

[11] Yu, K., X.L. Wang and Y. Zhou, , Underlying techniques for web services: a survey", Journal of Software, 15(3), 428. 2004

[12] IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, IEEE Std 1471-2000, September 2000

[13] Ministry of Defence Architecture Framework (MODAF), UK, version 1.2, http://www.modaf.org.uk accessed on 15 August 2008

[14] NATO Architecture Framework, version 3, AC/322- D0048. 2007

[15] Booth et al. Web Service Architecture. http://www.w3.org/tr/ws-arch/, W3C, Working Notes,, 2003/2004.36. In Sing et al. Designing Web Services with the J2EE 1.4 Platform. Addison-Wesley, 2004

[16] Keen et al. Patterns: Implementing an SOA using an Enterprise Service Bus. IBM Redbook, 22 July 2004

[17] Thomas Erl, Service-Oriented Architecture: A Field Guide to Integrating XML and Web Services, Published by Prentice Hall. 2004

[18] Aldis Cernicki - Mijic, Ante Martini, Integracija aplikacija u elektroprivredama 7. simpozij o sustavu vodenja EES-a Cavtat, Dubrovnik, 5. - 8. studenoga 2006

[19] Damir Pintar, Implementacija stvarnovremenskog skladištenja podataka na temelju principa integracije poslovnih aplikacija, http://www.fer.hr/_download/repository/kval_clanak_pintar.pdf, FER e-Campus. 05.06.2008

[20] "JSP777 Network Enabled Capability", Edition 1, Ministry of Defence, UK. http://www.mod.uk/NR/rdonlyres/E1403E7F-96FA-4550-AE14-4C7FF610FE3E/0/nec_jsp777.pdf, 2006
[21] "Exploring New Command and Control Concepts and Capabilities Final Report", NATO SAS-050, January 2006
[22] "Understanding Command and Control", Alberts D.S, and Hayes R.E., CCRP Publication Series, 2006
[23] "Power to the Edge, Command and Control in the Information Age", Alberts D.S., and Hayes R.E., CCRP Publication Series, 2005
[24] Draft UK Defence SOA Policy, JSP 602-1001, Draft Issue 2., March 2009
[25] Allied Rapid Reaction Corps, http://www.arrc.nato.int/, accessed on 17 April 2008
[26] A. Lazovik et al. Associating assertions with business processes and monitoring their execution. In: Proceedings of the Second International Conference on Service Oriented Computing, 2004
[27] e-Gov Project - Paves the way for modern Macedonia, http://www.egov.org.mk, consulted of January 2011
[28] Modeling SOA, IBM developerWorks, http://www.ibm.com/developerworks/rational/library/07/1002_amsden/index.html?S_TACT=105AGX15&S_CMP=LP , accessed on 21 April 2008
[29] OWL-S v1.2 Pre-release, http://www.ai.sri.com/daml/services/owl-s/1.2/, accessed on 19 August 2008
[30] "Get Serious About SOA Governance", BEA, September 2007
[31] Multilateral Interoperability Programme, http://www.mipsite.org/010_Public_Home_News.htm, accessed on 21 April 2008
[32] Dennis Medlow, Saab Systems: "Extending Service Orientated Architectures to the Deployed Land Environment"; Military Communications and Information Systems Conference(MilCis) Australia, http://www.milcis.com.au/, 2009
[33] OASIS. Reference Model for Service Oriented Architecture 1.0, http://docs.oasis-open.org/soa-rm/v1.0/ October 2006
[34] OASIS. Reference Architecture Foundation for Service Oriented Architecture Version 1.0 Committee Draft 02, http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/soa-ra-cd-02.pdf, 14 October 2009
[35] Eric Pulier, Hugh Taylor. Understanding Enterprise SOA, MANNING, 2006
[36] Judith Hurwitz, Robin Bloor,Carol Baroudi, Marcia Kaufman. Service Oriented Architecture for Dummies, WILEY, 2007
[37] Brigitte Anschuetz, Director, SOA WW Business Development & Client Engagement Management, IBM Software Group, Service Benefits – Life Beyond SOA, Military Communications and Information Systems Conference(MilCis) Australia, http://www.milcis.com.au/ 2009
[38] A. Candadai. A dynamic implementation framework for SOA-based applications. Web Logic Developers Journal: WLDJ, pp. 6-8, September/October, 2004
[39] D. Chappell. Enterprise Service Bus. O'Reilly Media, Inc., 2004
[40] Anis Char and Mira Mezini: "Hybrid web service composition: business processes meet business rules"; In: ICSOC '04: Proceedings of the 2nd international conference on Service oriented computing, pages 30-38, New York, NY, USA, ACM Press, 2004
[41] Scott Boag et al. Xquery 1.0: An XML query language,W3C working draft. Technical report, W3C, April, 2005

[42] Tung Bui and Alexandre Gachet. "Web services for negotiation and bargaining in electronic markets: Design requirements and implementation framework". Proceedings of the 38th Hawaii International Conference on System Sciences, IEEE, 2005
[43] David Burdett and Nickolas Kavantzas. "WSChoreography Model Overview". W3c working draft, W3C, March 2004
[44] Mr Murray Bruce and Mr Andy Heys: "Introducing the Triton SOA Foundation for Military Systems Integrators and Developers"; Military Communications and Information Systems Conference (MilCis), Australia, http://www.milcis.com.au/ 2010
[45] M.P. Papazoglou and P.M.A. Ribbers. e-Business: "Organizational and Technical Foundations"; John Wiley &Sons, Forthcoming 2005
[46] M.P. Papazoglou. "Extending the Service Oriented Architecture". Business Integration Journal, February 2005
[47] S. Kumar R. Rana. "Service on demand portals: A primer on federated portals". Web Logic Developers Journal:WLDJ, pages 22-24, September/October 2004
[48] D. Krafzig, K. Banke, and D. Slama. "Enterprise SOA:Service Oriented Architecture Best Practices". Prentice Hall, 2005
[49] Anjali Anagol-Subbaro. "J2EE Web Services on BEA WebLogic." Prentice Hall, Upper Saddle River, Newy Jersey, 2005
[50] G. Alonso, F. Casati, H. Kuno and V. Machiraju.Web Services: Concepts, Architectures and Applications.Springer, Heidelberg, Berlin, 2004
[51] A. Arora et al. "Web Services for Management (WS-Management)". Technical report, Advanced Micro Devices, Dell, Intel, Microsoft Corporation and Sun Microsystems, October, 2004
[52] Keith Ballinger et al. Web Services-Interoperability (WSI), Basic pro_le version 1.1, 2004-08-24. Technical report, WSI Organization (WS-I), 2004
[53] Abbie Barbir et al. Basic security pro_le, version 1.0. Technical report, Web Services-Interoperability Organization (WS-I), 2004
[54] J. Bloomberg. Events vs. services., ZapThink white paper, October 2004. available at: www.zapthink.com
[55] OASIS Web Services Business Process Execution Language, http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=wsbpel, accessed on 21 April 2011
[56] World Wide Web Consortium (W3C), http://www.w3.org/, accessed on 21 April 2011
[57] soapUI web services testing tool, http://www.soapui.org/ , accessed on 19 August 2011
[57] Jerry Mechling, Lecturer in Public Policy, Finnish Defense Forces – Network-Centric Operations, John F. Kennedy School of Governance, Harvard University, 2007 http://www-01.ibm.com/industries/government/ieg/pdf/finnish_defence_forces-nco.pdf
[58] M. Colan. Service-Oriented Architecture expands the vision of web services, Part 2. IBM DeveloperWorks, April 2004
[59] A. Dan et al. Web services on demand: WSLAdriven automated management. IBM Systems Journal, 43(1):136-158, March, 2004
[60] V. Deora et al. Incorporating QoS speci_cations in service discovery. In: Proceedings of WISE Workshops, Lecture Notes of Springer Verlag, 2004
[61] Arulazi Dhesiaseelan and Venkatavaradan Ragunathan. Web Services Container Reference Architecture (WSCRA). In: Proceedings of the International Conference on Web Services, IEEE, pages 806-805, 2004
[62] X. Ding et al Similarity search for web services. In:Proceedings of the 30th VLDB Conference, pages 372-383, 2004

[63] W3C. SOAP Version 1.2 Part 0: Primer (Second Edition),2007 http://www.w3.org/TR/2007/REC-soap12-part0-20070427/
[64] W3C. Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language, 2007, http://www.w3.org/TR/2007/REC-wsdl20-20070626
[65] Roy Thomas Fielding. PHD Thesis "Architectural Styles and the Design of Network-based Software Architectures", 2000 http://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf
[66] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. "Hypertext Transfer Protocol -- HTTP/1.1", The Internet Society 1999 http://www.w3.org/Protocols/rfc2616/rfc2616.html
[67] OASIS. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, 15 March 2005 http://docs.oasis-open.org/security/saml/v2.0/
[68] OASIS. eXtensible Access Control Markup Language (XACML) Version 2.0 OASIS Standard,1 Feb 2005, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
[69] OASIS. eXtensible Access Control Markup Language (XACML) Version 3.0 Committee Specification 01, 10 August 2010
[70] D. Chappell. "ESB myth busters: Clarity of de_nition for a growing phenomenon. Web Services" Journal, pages 22-26, February 2005
[71] S. Radcliffe, L. Trotman, and H. Duncan "Supporting Capability Evolution Using a Service Oriented Architecture Approach in a Military Command and Control Information System", http://nectise.com/pdfs/2_Stewart%20Radcliffe.pdf
[72] N. Brehm , J.M. Gómez,: Secure Web Service-based resource sharing in ERP networks. International Journal on Information Privacy and Security (JIPS) 1 pp. 29-48, 2005
[73] J. Achkoski, V. Trajkovik , and M. Dojcinovski "SOA Approach in Prototype of Intelligence Information System" ICT Innovations 2010, Web Proceedings, ISSN 1857-7288 pp. 149-160. 2010
[74] MuleSoft, http://mule.mulesource.org/display/MULE/Home, accessed on 19 August 2011.
[75] Protégé ontology editor tool, http://protege.stanford.edu/, accessed on 19 August 2011.
[76] SPARQL Query Language for RDF, W3C recommendation dated 15 January 2011.
[77] R.Podmore. D.Becker, R.Fairchild, M.Robinson, "Common Information Model – A Developer's Perspective", Proceedings of the 32nd Hawaii Internattional Conference on System Sciences, Volume 3, USA. 1999
[78] Torry Harris Business Solutions Inc. US, White Paper "Migration and Security in SOA", Distributed Systems & Services Group, University of Leeds, 03.03.2009, http://www.thbs.com/pdfs/Migration_and_Security_in_SOA.pdf, Consulted of April 19 2011
[79] Mukhtiar Memon, Michael Hafner, Ruth Breu. "Security as a Service - A Reference Architecture for SOA Security", Security in Information Systems, Proceedings of the 7th International Workshop on Security in Information Systems, WOSIS 2009, In conjunction with ICEIS 2009, Milan, Italy, May 2009. INSTICC Press 2009, ISBN 978-989-8111-91-3
[80] Hinton, H. Hondo, M. Hutchison, B.: "Security Patterns within a Service-oriented Architecture"; Nov. 2005, http://www.ibm.com/websphere/developer/services.
[81] Kannegati, R. Chodavarapu, P.: "SOA Security in Action"; Manning Publications Co., Greenwich, CT, USA, 2007
[82] Peterson, G.: "Service-oriented Security Indications for Use"; IEEE Security and Privacy, 7(2), 91–93, 2009.
[83] Michael Rosen, Marc J. Balcer, Boris Lublinsky, Kevin T. Smith: "Applied SOA: Service-Oriented Architecture and Design Strategies"; Wiley Publishing, Inc. 2008

[84] Harold F. Tipton, Micki Krause: "Information Security Management Handbook"; Sixth Edition, - Hardback 456 pages, Auerbach 2008.
[85] R. Breu, M. Hafner, F. Innerhofer-Oberperfler, and F. Wozak. Model-Driven Security Engineering of Service Oriented Systems. *Lecture Notes in Business Information Processing*, 5(5):59–71, 2008.
[86] F. Satoh et. al. "Methodology and Tools for End-to-End SOA Security Configurations". In Proceedinngs of the Conference *SERVICES '08*, pages 307–314, Honolulu, HI, 2008.
[87] M. Hafner. "SECTET A Domain Architecture for Model Driven Security"; PhD Thesis, November 2006.
[88] J.Lopez, J.A.Montenegro: "Specification and Design of Advanced Authentication Authorization Services"; Journal of Computer Standards and Interfaces, 27(5):467–478, 2005.
[89] M. Memon, M. Hafner, and R. Breu: "SECTISSIMO: A Platform-Independent Framework for Security Services". In *ModSec '08: MODELS 2008*, Toulouse, France, 2008.
[90] P.Niblett and S. Graham: "Events and service-oriented architecture: the OASIS web services notification specifications"; IBM System. Journal, 44(4):869–886, 2005.
[91] OASIS. WS-Trust Sepecifications, 2005. http://docs.oasis-open.org/.
[92] OASIS. Security Assertion Markup Language (SAML), 2005. http://www.oasis-open.org.
[93] Oracle. Service-Oriented Security: An Application-Centric Look at Identity Management, 2008. http://www.oracle.com/
[94] OASIS. WS-SecurityPolicy, 2007. http://docs.oasis-open.org/
[95] Joachim Biermann: "A Knowledge-Based Approach to Information Fusion for the Support of Military Intelligence, Military Data and Information Fusion"; RTO meeting proceedings MP-IST-040, Prague, Czech Republic, 20 to 22 October 2003.
[96] Joachim Biermann, Louis de Chantal, Reinert Korsnes, Jean Rohmer; Cagatay Uendeger: "From Unstructured to Structured Information in Military Intelligence: Some Steps to Improve Information Fusion"; SCI Panel Symposium, London, United Kingdom, 2004.
[97] Rud, D.; Schmietendorf, A.; Dumke, R.: "Product metrics for service-oriented infrastructures"; In Proceedings "16th International Workshop on Software Measurement/DASMA Metrik Kongress 2006" (IWSM/MetriKon 2006), pp. 161-174, , Potsdam, Germany, November 2-3, 2006
[98] Kunz, M.; Schmietendorf, A.; Dumke, R.; Wille, C.: "Towards a Service-Oriented Measurement Infrastructure"; Proceedings of the 3rd Software Measurement European Forum (SMEF), May 10-12, 2006, Rome, Italy, pp. 197-207
[99] Dejan Divac, Nikola Milivojević, Nenad Grujović, Vladimir Milivojević, Jelena Borota: "Service-Oriented Architecture of Modern Hydroinformation System"; In Proceedings of the 1st International Conference on Information Society Technology (ICIST 2011), Kopaonik, Serbia, March 6 - 9, 2011
[100] B. Elvesæter, A.J. Berre, A. Sadovykh: "Specifying Services using the Service oriented architecture Modeling Language (SoaML): A baseline for Specification of Cloud-based Services", the 1st International Conference on Cloud Computing and Service Science (CLOSER 2011), http://closer.scitevents.org/, 7-9 May 2011
[101] Gebhart, M., & Abeck, S.: "Metrics for Evaluating Service Designs based on SoaML"; International Journal on Advances in Software, 4(1&2), 61-75. Retrieved from http://iariajournals.org/software/, 2011

[102] Rud, D.; Schmietendorf, A.; Dumke, R.: Resource metrics for service-oriented infrastructures. In Proceedings "Workshop on Software Engineering Methods for Service Oriented Architecture 2007" (SEMSOA 2007), pp. 90-98, , Hannover, Germany, May 10-11, 2007

[103] Jugoslav Ackoski, Vladimir Trajkovik and Danco Davcev: "Service-Oriented Architecture Concept for Intelligence Information System Development"; The Third International Conferences on Advanced Service Computing SERVICE COMPUTATION 2011 (IARIA), Rome, Italy, September 25 - 30, 2011

[104] Gebhart M, Baumgartner M, Oehlert S, Blersch M And Abeck S: "Evaluation of Service Designs based on SoaML"; In Proceedings of the Fifth International Conference on Software Engineering Advances (ICSEA) (Hall J, Kaindl H, Lavazza L, Buchgeher G, And Takaki O), p 7, Nice, France. 2010

[105] NATO Standardization Agency (NSA): "AAP-6(2002) NATO Glossary of Terms and Definitions"; http://www.nato.int/docu/stanag/aap006/aap6.htm, 2002

[106] Jugoslav Ackoski, Vladimir Trajkovik: "Intelligence Information System Integration"; The 8th International Conference for Informatics and Information Technology (CIIT 2011), Bitola, Macedonia, March 2011

[107] Jugoslav Ackoski, Vladimir Trajkovik: "Intelligence Information System (IIS) with SOA-based Information Systems"; 33rd International Conference on Information Technology Interfaces, IEEE, Cavtat/Dubrovnik, Croatia, June 27 - 30, 2011

[108] Jugoslav Ackoski, Vladimir Trajkovik and Danco Davcev: "Security Issues for Intelligence Information System based on Service-Oriented Architecture"; International Conference ICT Innovations 2011, Skopje, Macedonia, September 14 – 16, 2011

[109] Jugoslav Achkoski, Vladimir Trajkovik and Metodija Dojchinovski: "An Intelligence Information System based on Service-Oriented Architecture: A Survey of Security Issues"; Information & Security: An International Journal, vol. 27: 91-111, 2011

[110] S. Maheswari, G. R. Karpagam: "QoS Based Efficient Web Service Selection"; European Journal of Scientific Research, vol. 66: 428-440, 2011

[111] Daniel A. Menascé: "Composing Web Services: A QoS View"; Journal IEEE Internet Computing, Vol. 8, No. 1, pp. 88-90, DOI: 10.1109/MIC.2004.57, 2004

[112] Huiyuan Zheng, Jian Yang, Weiliang Zhao: "QoS Probability Distribution Estimation forWeb Services and Service Compositions"; IEEE International Conference on Service-Oriented Computing and Applications, 2010 (SOCA), Perth, Australia, December 13-15, 2010

[113] Daniel A. Menascé: "Response-Time Analysis of Composite Web Services"; Journal IEEE Internet Computing, Vol. 8, No. 1., pp. 90-92, 2004

[114] Jin Sun Her, Si Won Choi, Sang Hun Oh, and Soo Dong Kim: "A Framework for Measuring Performance in Service-Oriented Architecture"; Third International Conference on Next Generation Web Services Practices, Seoul, South Korea, October 29 - 31, 2007

[115] Sravanthi Kalepu, Shonali Krishnaswamy, Seng Wai Loke: Verity: "A QoS Metric for Selecting Web Services and Providers"; Proceeding WISEW'03 Proceedings of the Fourth international conference on Web information systems engineering workshops IEEE Computer Society Washington, DC, USA, 2003

[116] Rifat M. Ramović: "Skripta - Pouzdanost sistema elektronskih, telekomunikacionih i informacionih"; Katedra za Mikroelektroniku I tehnicku fiziku, Univerzitet u Beogradu, Elektrotehnicki fakultet, 2005

[117] Wei Xie†, Hairong Sun‡, Yonghuan Cao† and Kishor S. Trivedi†: “Modeling of Online Service Availability Perceived by Web Users”