

УНИВЕРЗИТЕТ “СИНГИДУНУМ”



**Департман за
последипломске студије**

МАСТЕР СТУДИЈЕ

**СТУДИЈСКИ ПРОГРАМ:
САВРЕМЕНЕ ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ**

МАСТЕР РАД

**ИНФОРМАЦИОНИ СИСТЕМ ДИРЕКЦИЈЕ ЗА
УПРАВЉАЊЕ ОДУЗЕТОМ ИМОВИНОМ**



Ментор:

Проф.др Милан Милосављевић

Студент:

Ненад Ранковић, 410120/2012

Београд, април 2013.

С А Д Р Ж А Ј

САЖЕТАК	4
ABSTRACT	5
ИНФОРМАЦИОНИ СИСТЕМИ.....	6

I ПОГЛАВЉЕ

СОФТВЕРСКО РЕШЕЊЕ ИНФОРМАЦИОНОГ СИСТЕМА ДИРЕКЦИЈЕ ЗА УПРАВЉАЊЕ ОДУЗЕТОМ ИМОВИНОМ	12
УВОД У ИНФОРМАЦИОНЕ СИСТЕМЕ.....	12
1. АРХИТЕКТУРА СОФТВЕРСКОГ СИСТЕМА.....	13
2. КОРИШЋЕНЕ ТЕХНОЛОГИЈЕ	15
2.1 ADF FRAMEWORK	15
2.2 WEB LOGIC.....	16
2.3 ORACLE 11G БАЗА ПОДАТАКА.....	17
3. ИНСТАЛАЦИЈА СОФТВЕРА	19
3.1 ИНСТАЛАЦИЈА БАЗЕ ПОДАТАКА.....	19
3.2 DEPLOY АПЛИКАЦИЈЕ НА WEBLOGIC	19
3.3 ИНСТАЛАЦИЈА КЛИЈЕНТА.....	23

II ПОГЛАВЉЕ

4. ХАРДВЕРСКЕ КОМПОНЕНТЕ КОЈЕ СУ УГРАЂЕНЕ У СИСТЕМ ДИРЕКЦИЈЕ ЗА УПРАВЉАЊЕ ОДУЗЕТОМ ИМОВИНОМ	27
4.1 ПЕРИФЕРНА ОПРЕМА	27
4.2 ХАРДВЕР И СИСТЕМСКИ СОФТВЕР.....	28
5. ТЕХНИЧКЕ КАРАКТЕРИСТИКЕ ХАРДВЕРСКИХ КОМПОНЕНТИ	29
5.1 ЛАПТОП -FTS LIFEBOOK A531	29
5.2 МОБИЛНИ ШТАМПАЧ -CANNON PIXMA IP100	30
5.3 СКЕНЕР VELIKOG КАПАЦИТЕТА CANNON DR7750C	31
5.4 МРЕЖНИ ШТАМПАЧ -CANNON LBP6300DN.....	32
5.5 РАДНА СТАНИЦА FTS ESPRIMO E500 E85+.....	33
5.6 СЕРВЕР FTS PY RX300S6 8x2.5 gold PSU.....	34
5.7 СИСТЕМ ЗА ЧУВАЊЕ ПОДАТАКА FTS ETERNUS DX80 S2.....	37

5.8. КОНЦЕНТРАТОРИ МРЕЖЕ Mikrotik RB1100AH.....	40
5.9 19” СЕРВЕРСКИ ОРМАР FTS PRIMECENTER M1 Rack 742A 42U-1050x700 ..	41

III ПОГЛАВЉЕ

6. ЗАШТИТА ИНФОРМАЦИОНОГ СИСТЕМА ДИРЕКЦИЈЕ ЗА УПРАВЉАЊЕ ОДУЗЕТОМ ИМОВИНОМ	43
6.1 ЕЛЕКТОНСКО ПОСЛОВАЊЕ И БЕЗБЕДНОСТ ИНФОРМАЦИОНИХ СИСТЕМА	43
6.2 БЕЗБЕДНОСТ.....	44
6.3 СТАНДАРДИ.....	49
6.4 ЗАШТИТА СИСТЕМА У ПРАВОСУЂУ.....	52
6.5 БЕЗБЕДНОСТ КАО СТРАТЕШКО ОПРЕДЕЉЕЊЕ.....	54
6.6 СТАНДАРД БЕЗБЕДНОСТИ ISO 27001.....	57
6.7 ПОЛИТИКА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ У ПРАВОСУЂУ.....	61
6.8 ПРЕПОРУКЕ ЗА МОНИТОРИНГ БАЗА ПОДАТАКА	65
6.9 ПРЕДЛОГ ЗА ПОБОЉШАЊЕ ЗАШТИТЕ ИНФОРМАЦИОНОГ СИСТЕМА.....	69

<u>ЗАКЉУЧАК</u>	70
------------------------------	-----------

<u>ЛИТЕРАТУРА</u>	71
--------------------------------	-----------

САЖЕТАК:

Правосудни информациони систем у Републици Србији, који се развија са свим специфичностима карактеристичним за правосуђе као посебну грану власти, својом структуром обухвата веома сложене пословне процесе, пословне функције, догађаје, анализе и проблеме као и друге специфичности по питању тока података који егзистирају у систему. Као такав јесте велики изазов за послове заштите од недозвољених радњи и злоупотреба. У овом раду приказане су смернице за повећање степена безбедности као и софтвер, хардвер који се користе у једном Правосудном органу. Сам рад се састоји из 3 целине које имају за циљ да нам да нам приближе функционисање информационог система Дирекције за управљање одузетом имовином. Целине које чине овај рад су :

- Поглавље I : Софтверко решење информационог система Дирекције за управљање одузетом имовином
- Поглавље II : Хардверко решење информационог система Дирекције за управљање одузетом имовином
- Поглавље III : Заштита информационог система Дирекције за управљање одузетом имовином

У самом раду ћемо се детаљно позабавити проблемима и погодностима које пружа један савремени информациони систем.

ABSTRACT :

Judicial Information System in the Republic of Serbia, which is being developed with all the specific characteristics of the judiciary as a separate branch of government, its structure includes a very complex business processes, business functions, events, and analyzes problems and other specifics about the flow of data existing in the system. As such, it is a great challenge for safety of unauthorized activities and fraud. This paper presents the guidelines to increase the level of safety as well as software, hardware used in a judicial body. The work consists of three parts which are intended to reach out to us that our operation of the information system of the Directorate for the management of seized assets. Units that make up this paper are :

- Chapter I: Softversko information system solution Directorate for Management of Seized Assets
- Chapter II: Hardversko information system solution agency for the management of seized assets
- Chapter III: Environmental Information Systems Directorate for Management of Seized Assets

In the paper, we will address the issues in detail and the advantages offered by a modern information system.

Информациони систем

Информациони систем се може дефинисати као систем у коме се везе између објеката и везе система са околином остварују разменом информација[1].

Предмет нашег истраживања су софтвер, хардвер, и заштита информационог систем Министарства правде и државне управе –Дирекције за управљање одузетом имовином. Информациони систем је уређени скуп података, процеса интерфејса, мрежа, технологија и људи који су у међусобној корелацији у циљу подршке и побољшања свакодневних пословних операција.

У истраживању полазимо од хипотезе : Информациони систем који ми истражујемо је дефинисан својом мисијом и визијом.

Мисија Информационог система за одузимање имовине је што већа аутоматизација пословних процеса и прецизна евиденција одузете имовине.

Визија Информационог система за одузимање имовине је :

- Уз минималне трошкове одржавања да се очува вредност одузете имовине
- Да управљање одузетом имовином омогући остварење прихода од те имовине
- Прецизнија и ефикаснија евиденција о одузетој имовини

Овај мастер рад чини 3 целине која за циљ имају да нам приближе функционисање информационог система Дирекције за управљање одузетом имовином. Мастер рад је конспиран на следећи начин:

- АПСТРАКТ
- Поглавље I : Софтверко решење информационог система Дирекције за управљање одузетом имовином
- Поглавље II : Хардверко решење информационог система Дирекције за управљање одузетом имовином
- Поглавље III : Заштита информационог система Дирекције за управљање одузетом имовином

Нашу генералну хипотетичку тврдњу операционализујемо преко:

Уводни део о информационим системима

- **Hardware** рачунарског система чини материјално-техничка компонента информационог система, односно физичке јединице рачунарског система намењене процесирању и преносу података.
- **Појам софтвер** односи се на свеукупност инструкција, програма и процедура који се генерише, активира и користи на разновразне начине да би омогућио хардверу да реализује жеијене послове. Софтвер се састоји од података смештених на магнетним медијумима у електронским меморијама итд..[2]

Хардверске компоненте које су уграђене у информациони систем Дирекције за управљање одузетом имовином

Hardver су уређаји рачунара али и друге телекомуникационе опреме. Можда најједноставнија дефиниција hardvera је да је - хардвер све што је опипљиво или додирљиво (за разлику одсофтвера). [3]

Техничке карактеристике хардверских компоненти -

Hardver представља техничка опрема рачунара тј. Hardver чине техничке и електронске компоненте рачунара.

Функција хардверских компоненти у раду информационог система

Чине:

- механички,
- електронски,
- магнетни и оптички
- делови у које спадају компоненте централног рачунара и терминала,
- компоненте за повезивање рачунара и др

ПОЈАМ СОФТВЕРА

АРХИТЕКТУРА СОФТВЕРСКОГ СИСТЕМА БРЕЗА ЕРП

Да би се одређени пословни софтвер могао користити готово увек је потребно упознати архитектуру система који се инсталира, стећи одређена уводна знања о технологијама и осталим градивним елементима система. Архитектуром софтверског система ЕРП је основа софтвера за Одузимање имовине [4].

➤ КОРИШЋЕНЕ ТЕХНОЛОГИЈЕ

Ради лакшег сагледавања како један информациони систем функционише морамо се прво упознати са технологијама које су коришћене у изради тог система.

➤ ИНСТАЛАЦИЈА СОФТВЕРА

Инсталација софтвера укључује :

- Генерисање структуре базе података
- Поставка апликације на Weblogic server
- Инсталација клијента

Циљ нашег истраживања је научни и друштвени.

Нучни циљ је усмерен ка научној дескрипцији и опису то јест изради и оперативности информационог система као и функцији и структури истог.

Друштвени циљ је усмерен на аутоматизацији пословних процеса а резултат аутоматизације је што боља експлоатација одузете имовине уз минималне трошкове.

Систем хипотеза:

Наш информациони систем нас је определио на дијалектички приступ као и примену основних синтетичких и аналитичких метода, а од опште-научних метода хипотетичке дедуктивне као и од метода и техника прикупљања података.

Најбитније функције информационог система [5]:

- Функција информисања
- Функција документовања

Функција информисања

Многи аутори сматрају да је Информациони систем одређени скуп метода, поступака и ресурса, обликованих тако да се потпомогне постизање неких циљева. Информациони систем својим информисањем осигурава релевантне информације за оперативно и развојно управљање организацијом [6]. То имплицира да се функција информисања остварује у сврху управљања организацијом, док је функција управљања, као хијерархијски највиша функција организације, по својој суштини, такође, информациони процес. Из тог разлога је функција информисања од фундаменталног значаја за оцјену квалитета информационог система. Највиши ниво развијености имају компјутеризовани информациони системи који су оријентисани на подршку одлучивању и управљању.

Функција документовања

За све активности организације неопходно је обезбедити документациону подлогу путем информационог система[7]. Документациона подлога, односно документација, је резултат потреба и захтева субјеката из окружења, јер она чини контролу и размјену информација уопште. Такође је неопходно обезбиједити могућност ревизије пословања у сваком тренутку како би се могли реконструисати пословни догађаји.

Основни подаци о Дирекцији за управљање одузетом имовином

- Адреса: Немањина 22-26
- Поштански број и град: 11000 Београд
- Општина: Савски венац
- Шифра делатности:8411
- Број жиро рачуна: 840-1620-21
- Матични број: 17766830
- ПИБ: 105952373

Дирекција за управљање одузетом имовином је почела са радом ступањем на снагу Закона о одузимању имовине проистекле из кривичног дела („Сл. гласник РС“, бр. 97/2008) 01. марта 2009. године. Одредбом члана 8. став 1. истог закона основана је као орган у саставу Министарства правде [8]. Надлежност Дирекције за управљање одузетом имовином уређена је чланом 9. Закона о одузимању имовине проистекле из кривичног дела ("Службени гласник РС", број 97/2008), којим је прописано да Дирекција за управљање одузетом имовином обавља послове, који се односе на: управљање одузетом имовином проистеклом из кривичног дела, предметима кривичног дела, имовинском користи прибављеном кривичним делом и имовином датом на име јемства у кривичном поступку; стручну процену одузете имовине проистекле из кривичног дела; складиштење, чување и продају привремено одузете имовине проистекле из кривичног дела, као и располагање тако добијеним средствима, у складу са законом; вођење евиденције о имовини, којом се управља и о судским поступцима, у којима је одлучивано о таквој имовини; учешће у пружању међународне правне помоћи; учествовање у обуци државних службеника и носилаца правосудних функција, у вези са одузимањем имовине проистекле из кривичног дела; послови у вези са имовинском користи проистеклом из привредног преступа, односно прекршаја; обавља и друге послове, у складу са овим законом [9].

ОПШТИ ПОЈМОВИ КОРИШЋЕНИ У РАДУ

- ADF – Application Development Fusion
- ERP – Enterprise Resource Planning
- СУБП – Систем за управљање базом података
- JVM – Java Virtual Machine
- XML – Extensible Markup Language
- HTTP – HyperText Transfer Protocol
- JAVA EE – Java Enterprise Edition
- DDL – Data Definition Language
- DML – Data Manipulation Language

I ПОГЛАВЉЕ

СОФТВЕРСКО РЕШЕЊЕ ИНФОРМАЦИОНОГ СИСТЕМА ДИРЕКЦИЈЕ ЗА УПРАВЉАЊЕ ОДУЗЕТОМ ИМОВИНОМ

Увод у информационе системе

Да би се одређени пословни софтвер могао користити готово увек је потребно упознати архитектуру система који се инсталира, стећи одређена уводна знања о технологијама и осталим градивним елементима система, а затим и спровести правилну инсталацију и поставку (eng. deploy) софтвера[10].

У овом документу је извршен пролазак кроз све претходно набројане ставке како би се што лакше и што брже могло доћи до радне верзије софтвера (eng. Runtime version) за Одузимање имовине.

Прво поглавље упознаје нас са архитектуром софтверског система ЕРП који је основа софтвера за Одузимање имовине.

У другом поглављу се могу стећи основна знања о апликацијама и технологијама којима би требало овладати да би се могло ваљано управљати радном верзијом софтвера. Дат је опис појединачно за ADF Framwork, Weblogic server i Oracle 11g базу података.

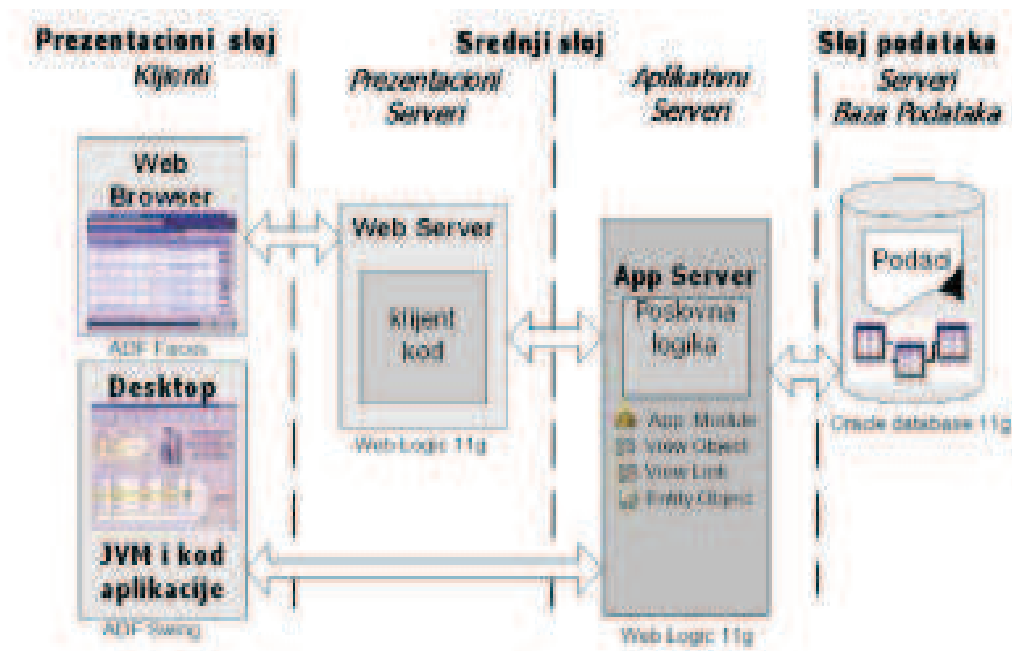
После основног упознавања са технологијама у трећем поглављу је дато упутство за инсталацију софтвера Одузета имовина који укључује: генерисање структуре базе података, поставка апликације на Weblogic server и инсталација клијента.

➤ АРХИТЕКТУРА СОФТВЕРСКОГ СИСТЕМА ЕРП

Enterprise Resource Planning (ЕРП) системи су једни од најкомплекснијих, најопширнијих и најкориснијих постојећих информационих система. Мултимодуларност и мултиапликативност су главна одлика ЕРП-ова која им омогућава примену у пословним системима свих величина као и корекцију њихове величине у зависности од потреба специфичних компанија. ЕРП системи покушавају да покрију све главне функције компаније било да се ради о комерцијалним, непрофитним, друштвеним или услужним делатностима.

ЕРП је производ који је први пут развијен и примењен 1993. године. Од тада је даље усавршаван и прилагођен напретку у информационом технологијима и потребама привреде. У 2002. години је преведен у трослојно Oracle JAVA XML окружење које представља прелазак на ЕРП 2 стандард.

Архитектура информационог система Дирекција за управљање одузетом имовином приказана је на слици 1. [11]



Слика 1: Трослојна ЕРП архитектура

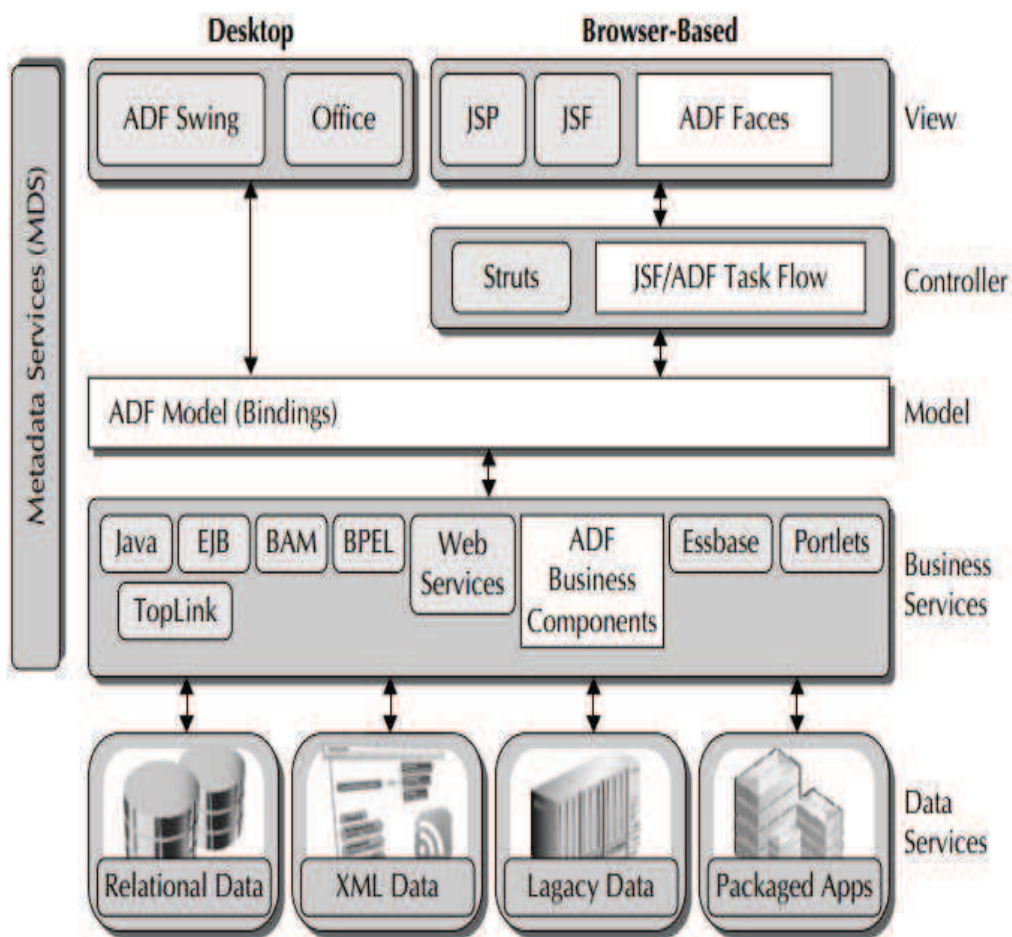
Као што се види на слици трослојне архитектуре, клијенте ЕРП система је могуће покренути у независном Десктоп окружењу, као и из Web Browser-а. Средњи слој се састоји од презентационог и апликативних сервера који могу да остваре комуникацију без обзира на начин на који су имплементирани. На дну трослојне архитектуре се налазе сервери база података који су базирани на Oracle 11g систему за управљање базама података. ЕРП решење је прилагођено потребама домаће привреде, па самим тим аутоматизује највећи део пословних процеса који се могу у њима наћи. С обзиром на чињеницу да је ЕРП јединствено софтверско решење, може се рећи да компаније у једном пакету добијају интегрисано комплетно функционисање свог пословног система. Као и највећи светски ЕРП системи и ЕРП Одузимање имовине подржава модуларну имплементацију и проширивост. Основни задатак сваке озбиљне софтверске архитектуре је да омогући максималну флексибилност и проширивост [12]. Последња реченица је и главни разлог због кога је коришћењем ЕРП-а направљена апликација „Одузета имовина“ која је имплементирана као посебан модул. Важно је напоменути да је као клијент у софтверу „Одузета имовина“ коришћена имплементација ADF Swing фрејмворка што значи да је клијент JAVA desktop апликација. Клијент комуницира са Web Logic сервером (који представља интегрално решење за Web и Апликативни сервер). У основи комплетног система се налази Oracle 11g база података.

► КОРИШЋЕНЕ ТЕХНОЛОГИЈЕ

За сваку од коришћених технологија у посебном поглављу су дате основе како би боље приближиле администратору софтвера "Одузета имовина".

2.1 ADF FRAMEWORK

Архитектура ADF Framework који се у нашем случају користи за табеле у бази података Пример Слика 2 . [13]



Слика 2: ADF Framework архитектура

За многе кориснике рачунара ADF Framework представља непознаницу иако су га вероватно много пута користили кроз свој редован рад са бројним Oracle-овим апликацијама које су углавном базиране на овом решењу. У основи улога ADF

Framework-a je da obezbedi fleksibilnu mogućnost apstrakcije nižih nivoa softvera, u ovom slučaju tabela u bazi podataka.

Za razliku od drugih okruženja ADF Framework ima već ugrađenu podršku za konekciju na bazu, keširanje sloгова, управљање трансакцијама базе података, валидацију и приказ на монитору.

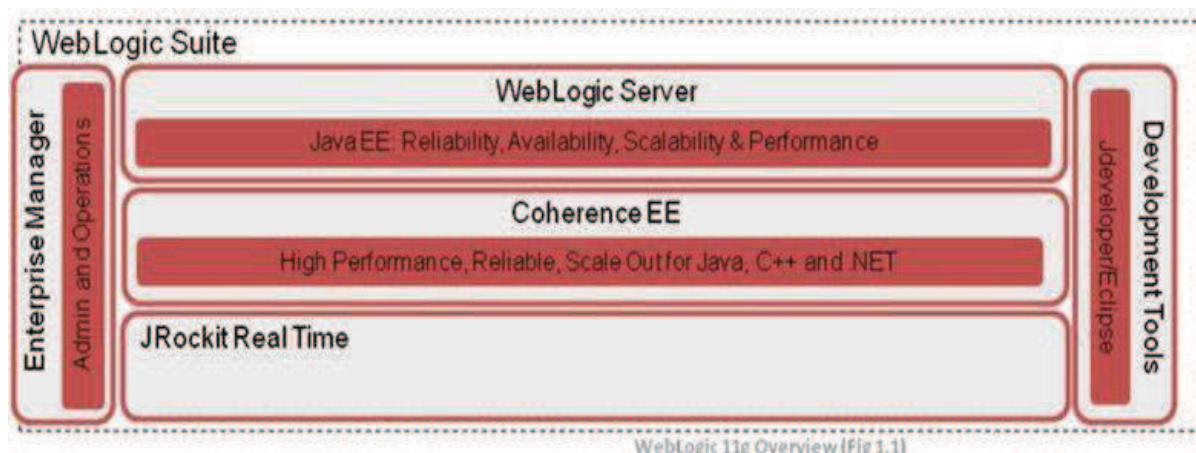
Као што се може приметити на Слици 2. ADF Framework у себи садржи имплементирано много различитих технологија и стандарда. Најважније је приметити и његову одабрану трослојну архитектуру која се зове Model-View-Controller [14]. У најкраћем ова архитектура подразумева раздвајање модела базе података, пословне логике и корисничког интерфејса на посебне слојеве како би се олакшао развој и одржавање софтвера.

2.2 WEB LOGIC

Oracle Weblogic 11g сервер представља JAVA EE платформу која укључује неколико различитих алата и софтвера од којих су за нас најважнији: апликативни сервер и веб сервер. Weblogic 11g апликативни сервер је један од водећих апликативних сервера на тржишту. Оно што га издваја у односу на конкуренцију су робустност, скалабилност и зрелост. Инсталација и постављање пословних информационих система и портала су знатно олакшана на овом апликативном серверу, а поред тога могуће је извршити ове акције на више начина: deploy .ear фајла, инсталација директно из развојног окружења или из посебно испрограмираног инсталера.

Weblogic 11g је базиран на JAVA програмском језику и апликацијама које су инсталиране на њему обезбеђује различите сервисе: управљање сесијама, заштита, дистрибуирано именовање, приступ бази података, перзистентност и многе друге. Могуће га је инсталирати на различитим оперативним системима и платформама: Windows, Solaris, Linux, Unix, IBM AIX...

Weblogic 11g обезbeđuje različite servise: upravljanje sesijama, zaštita, distribuirano imenovanje, pristup bazi podataka, perzistentnost primer prikazan na slici 3. [15]

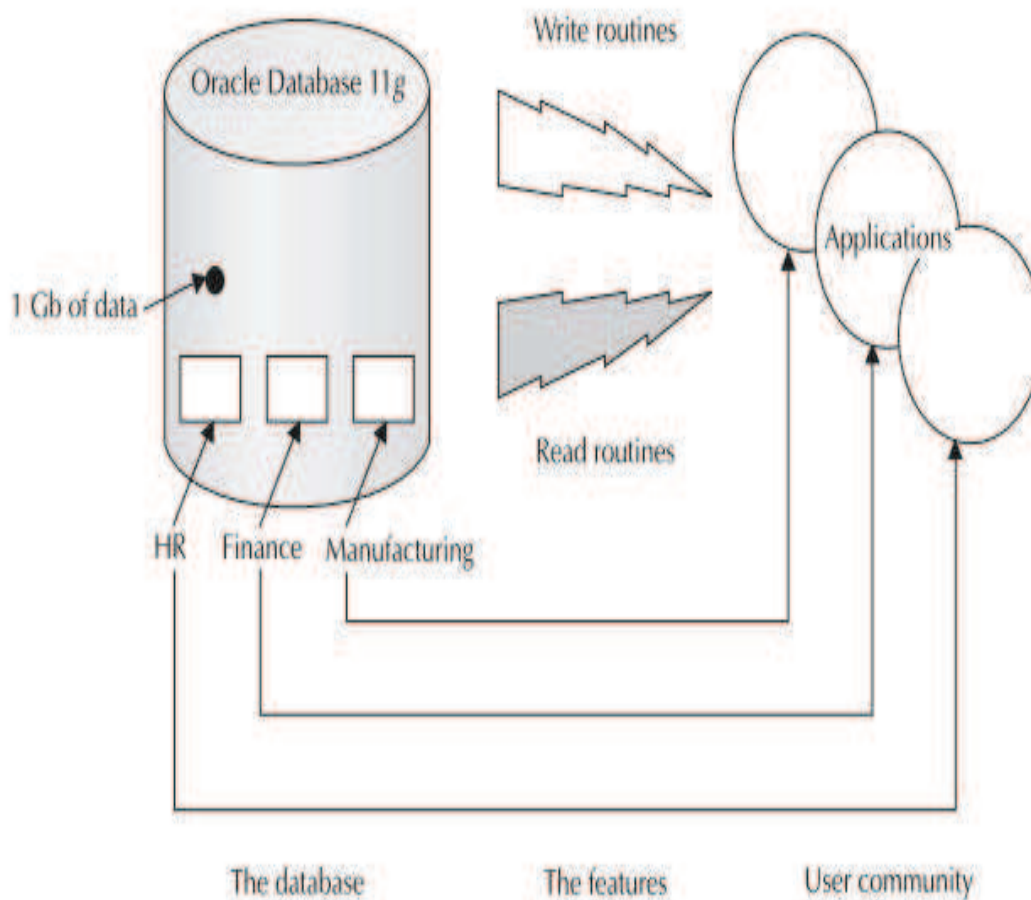


Слика 3: WEB LOGIC 11g платформа

2.3 ORACLE 11G БАЗА ПОДАТАКА

Oracle 11G база података је најмодернији тип система за управљање базама података (СУБП) који долази из компаније Oracle. Намера овог софтвера је да унапреди и прошири могућности смештања података у велике базе података за различите типове компанија. База података треба да омогући брзо добијање података по захтеву корисника по политици „упиши једном, читај више пута“ како би се ресурси правилно искористили. Релационе базе података управо то омогућавају ако су правилно моделиране и структуриране.

Пример Употребе релационе базе података Oracle Database 11g приказано на слици 4 . [16]



Слика 4: Употреба релационе базе података Oracle Database 11g

Табеле су носиоци података у овој базу и омогућене су основне и додатне DDL i DML команде, као и употреба језика PL/SQL који постоји само у Oracle базама података. Помоћу SQL упита који ће се извршавати било у окружењу командне јединице или из неког графичког окружења корисник базе може додавати, ажурирати, брисати слогове и извучити различите врсте везаних података. Поузданост је такође јача страна овог софтвера, као и скалабилност.

3. ИНСТАЛАЦИЈА СОФТВЕРА

У овом делу биће описана процедура инсталације и постављања софтверског пакета „Одузета имовина“.

3.1.ИНСТАЛАЦИЈА БАЗЕ ПОДАТАКА

За инсталацију базе података потребно је покренути инсталационе скрипте са SQL кодом из командне линије (Command Prompt).

Пример инсталације базе података приказан на слици 5.

```
C:\>imp full=y file=C:\exportFullMinistarstvo.rar
```

Слика 5: Команда за инсталацију базе података

3.2 DEPLOY АПЛИКАЦИЈЕ НА WEBLOGIC

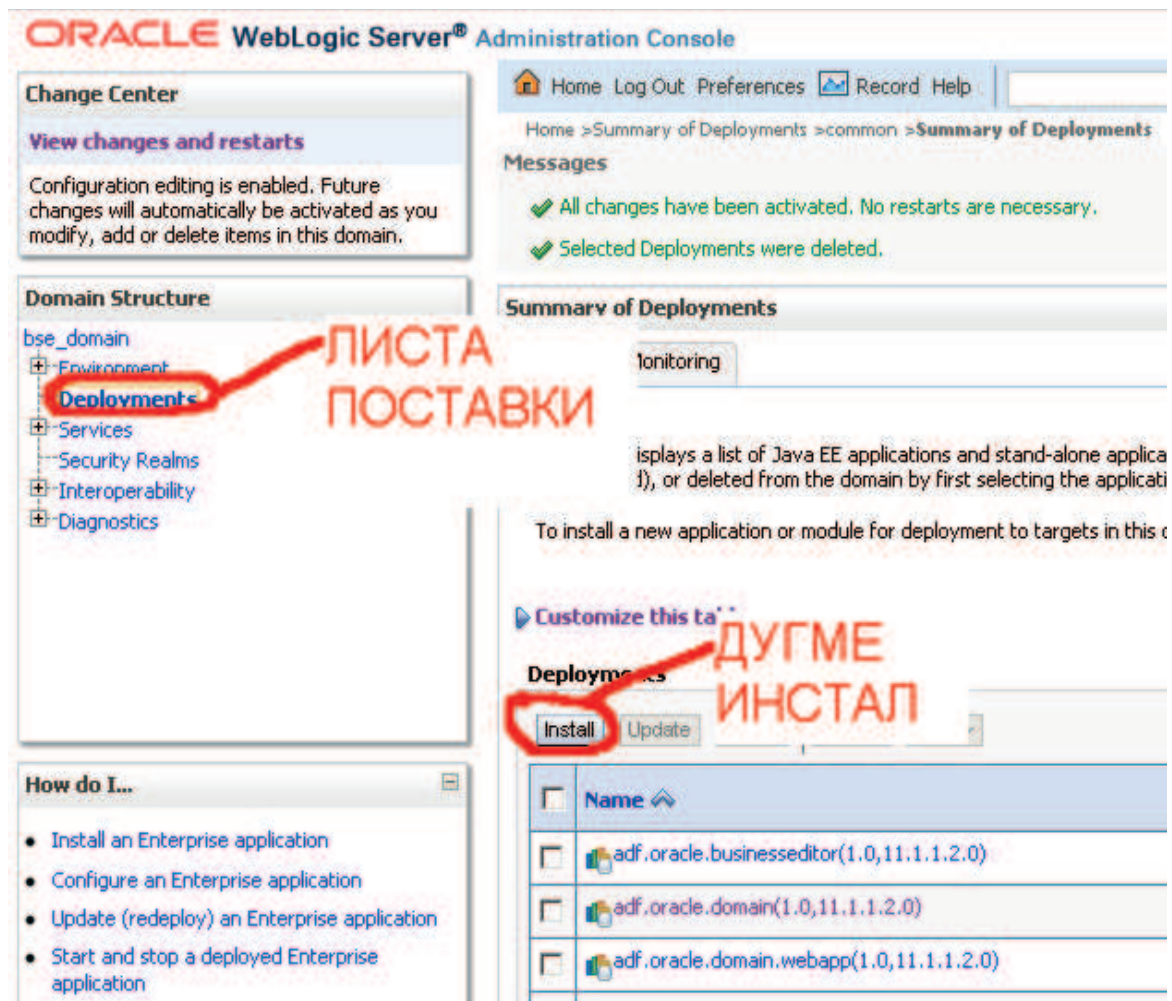
Да би се апликације уопште могле користити потребно је поставити JAVA извршне фајлове на Weblogic 11g сервер. С обзиром на чињеницу да у Одузимање имовине ЕРП-у постоји више апликација које користе различите библиотеке разликујемо два типа поставки:

- 1) Поставка спољне библиотеке (било која библиотека која није део ADF-а екстензија .jar),
- 2) Поставка пословне апликације (екстензија .ear).

Важно је напоменути да је за сваки JAVA извршни фајл потребно извршити поставку само једном у одређеној верзији. У случају изласка нове верзије софтвера инсталација и поставка се врши од почетка само за извршни фајл који је измењен.

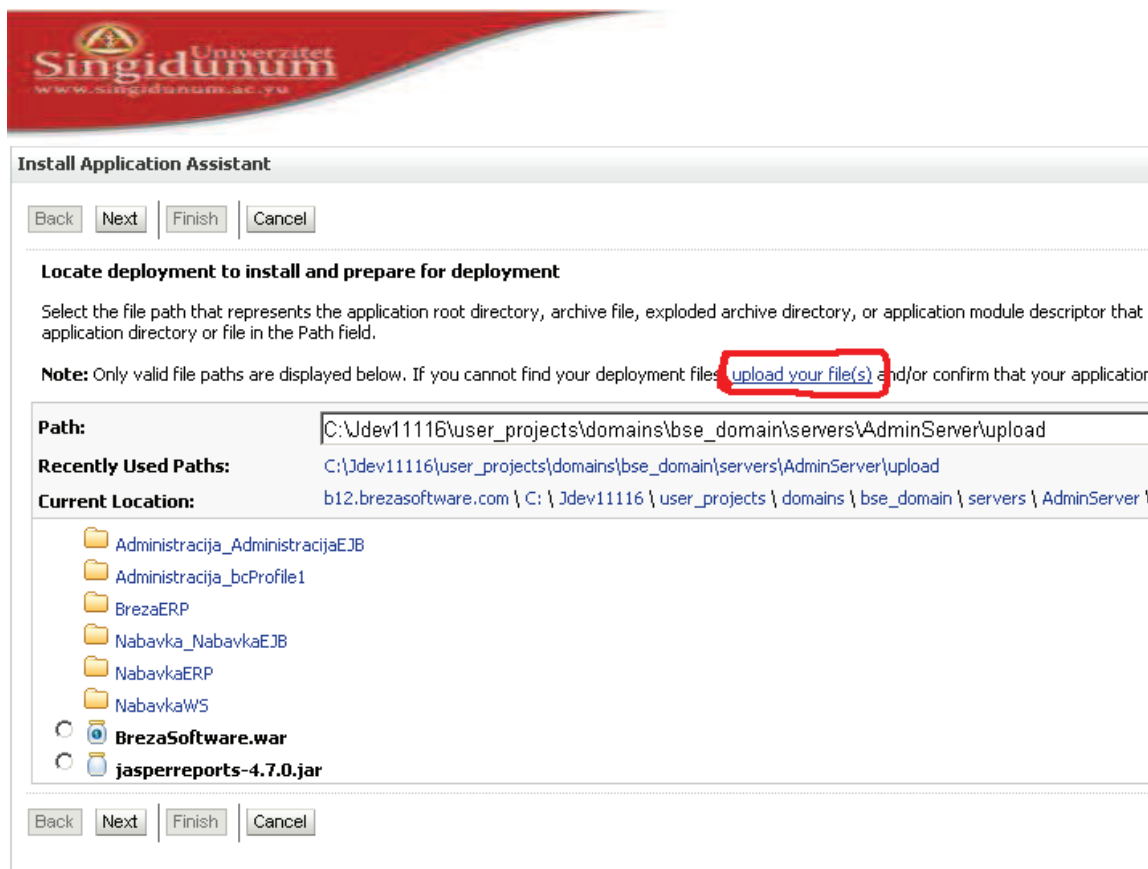
Поставка спољне библиотеке (.jar екстензија) се врши на следећи начин (дат је пример за библиотеку common.jar):

Пример постављања спољне библиотеке приказан је сегментно на сликама 6, 7, 8, 9, 10.



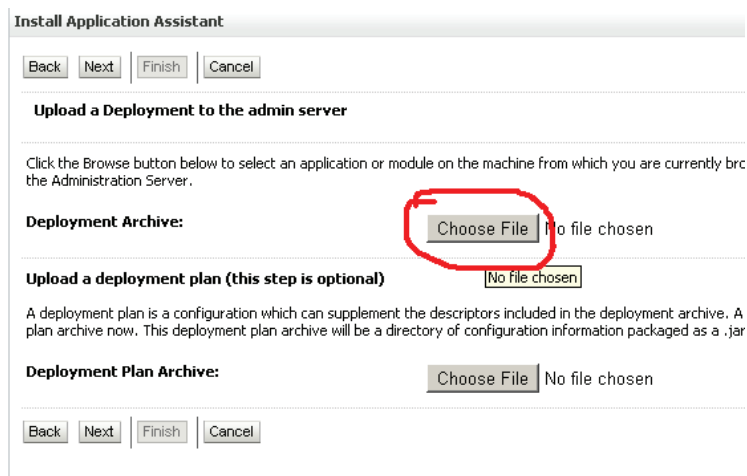
Слика 6: Показује листу поставки и опцију за инсталацију спољне библиотеке

Уласком у административну конзолу WebLogic Server-а потребно је изабрати опцију **Deployment** која ће вратити са десне стране листу поставки библиотека и апликација. Затим је потребно кликнути на дугме **Install** како би се отворила нова страница за инсталацију и постављање библиотеке.



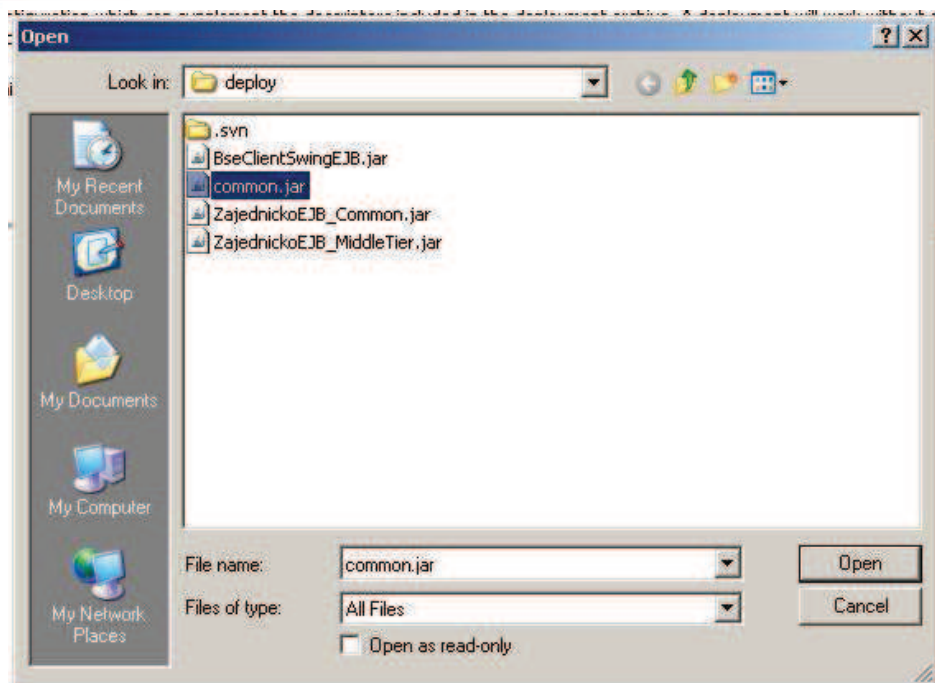
Слика 7: отварање странице за избор жељене библиотеке

На следећој страници потребно је изабрати подвучени линк (upload your file) како би се приступило избору жељене библиотеке.



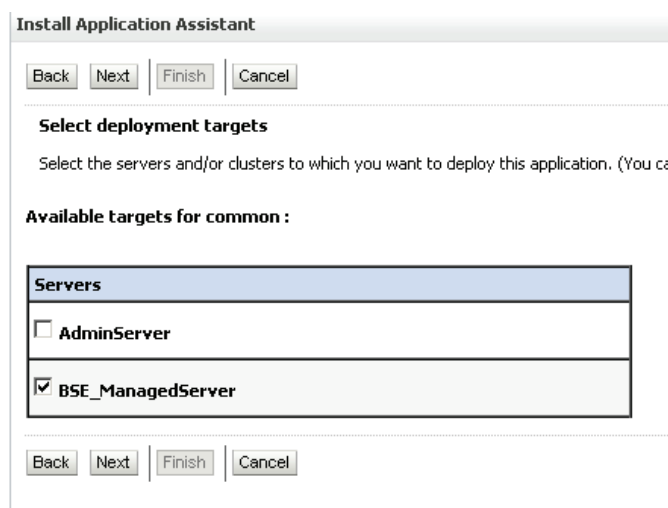
Слика 8: страница за приступање библиотеци

Сада треба кликнути на дугме Choose File које стоји после текста Deployment Archive.



Слика 9: Претрага и селектовање жељене библиотеке

Из прозора за одабир фајлова изабрати жељену библиотеку (common.jar у овом случају) и притиснути дугме **Open** . Затим на страници на коју се вратимо треба да изаберемо **Next**.

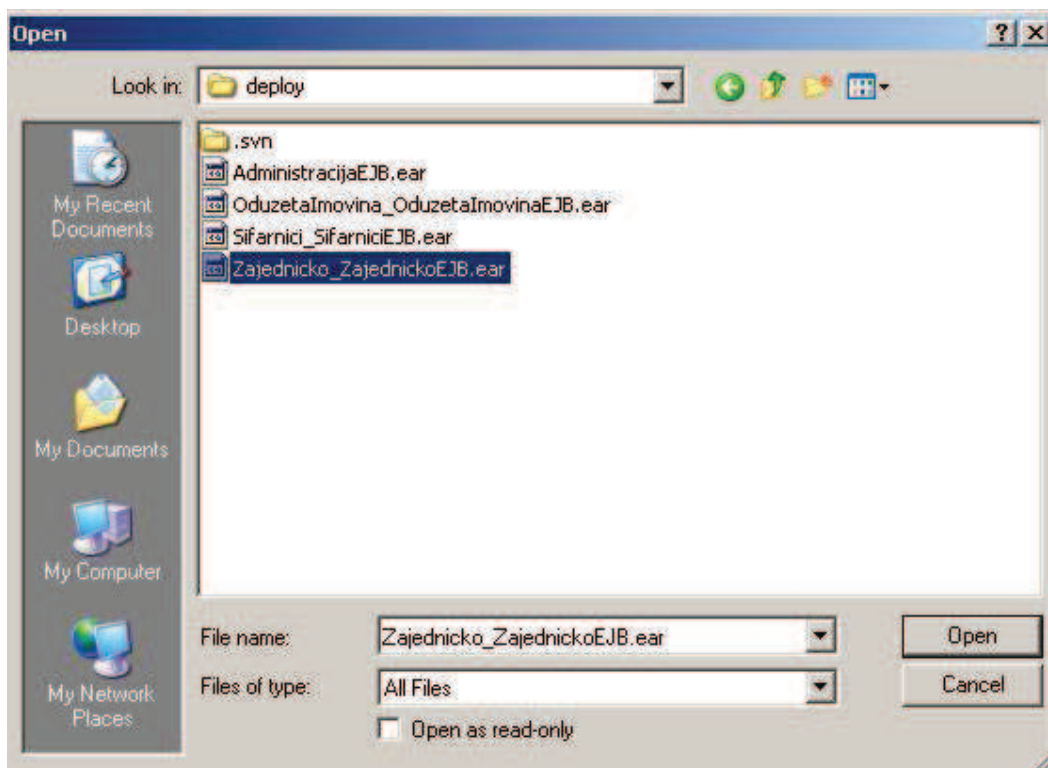


Слика 10: Одабир сервера на ком ће библиотека да се инсталира

У новом прозору потребно је изабрати сервер на ком ће библиотека бити инсталирана и затим опет кликнути на дугмић **Next**. На последњој страници се добија обавештење да је инсталација прошла у реду и потребно је кликнути на дугме **Finish** .

Инсталација апликација се спроводи на индентичан начин осим што на Слици 9 изаберемо фајл са екстензијом **.ear**.

Апликација се налази у фолдеру **deploy** пример на Слици 11.



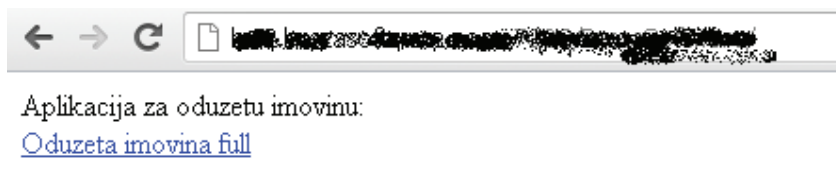
Слика 11: Селектовање фајла Апликације

Све библиотеке које је потребно инсталирати налазе се у фолдеру **biblioteke**, а апликације у фолдеру **deploy**. Након постављања апликација и библиотеке на сервер може се прећи на инсталацију програма на клијентским машинама.

3.3 ИНСТАЛАЦИЈА КЛИЈЕНТА

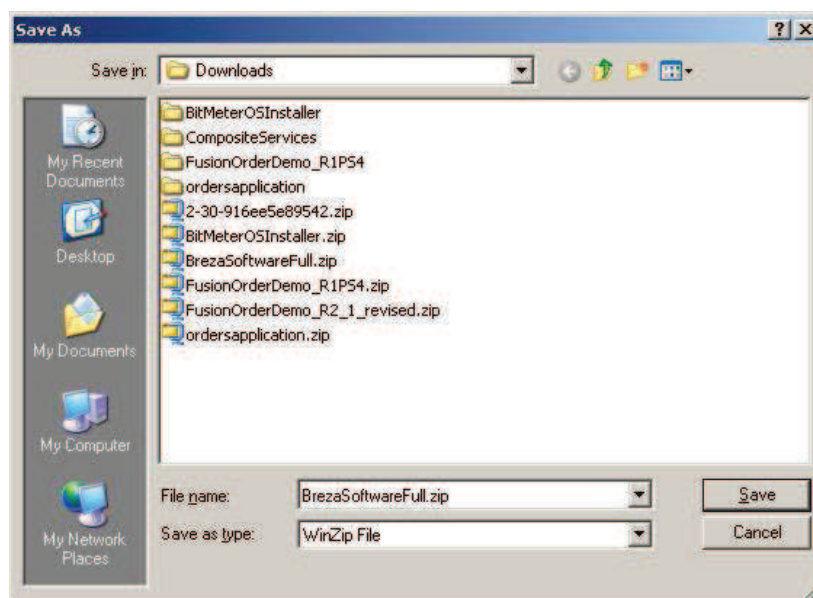
Инсталација клијента се обавља изузетно једноставно. Потребно је у Интернет прегледачу укуцати адресу сервера (која ће бити саопштена корисницима апликације након инсталације сервера) и кликнути на линк [Oduzeta imovina full](#).

Пример инсталације клијената преко адресе сервера Слика 12.



Слика 12: Инсталација клијента

Када кликнемо на „ [Oduzeta imovina full](#) ” појавиће нам се прозор на коме је потребно да селекујемо „ SoftwareFull.zip ” после селектовања одредимо место где ће се налазити клијент инсталација пример приказан на Слици 13.



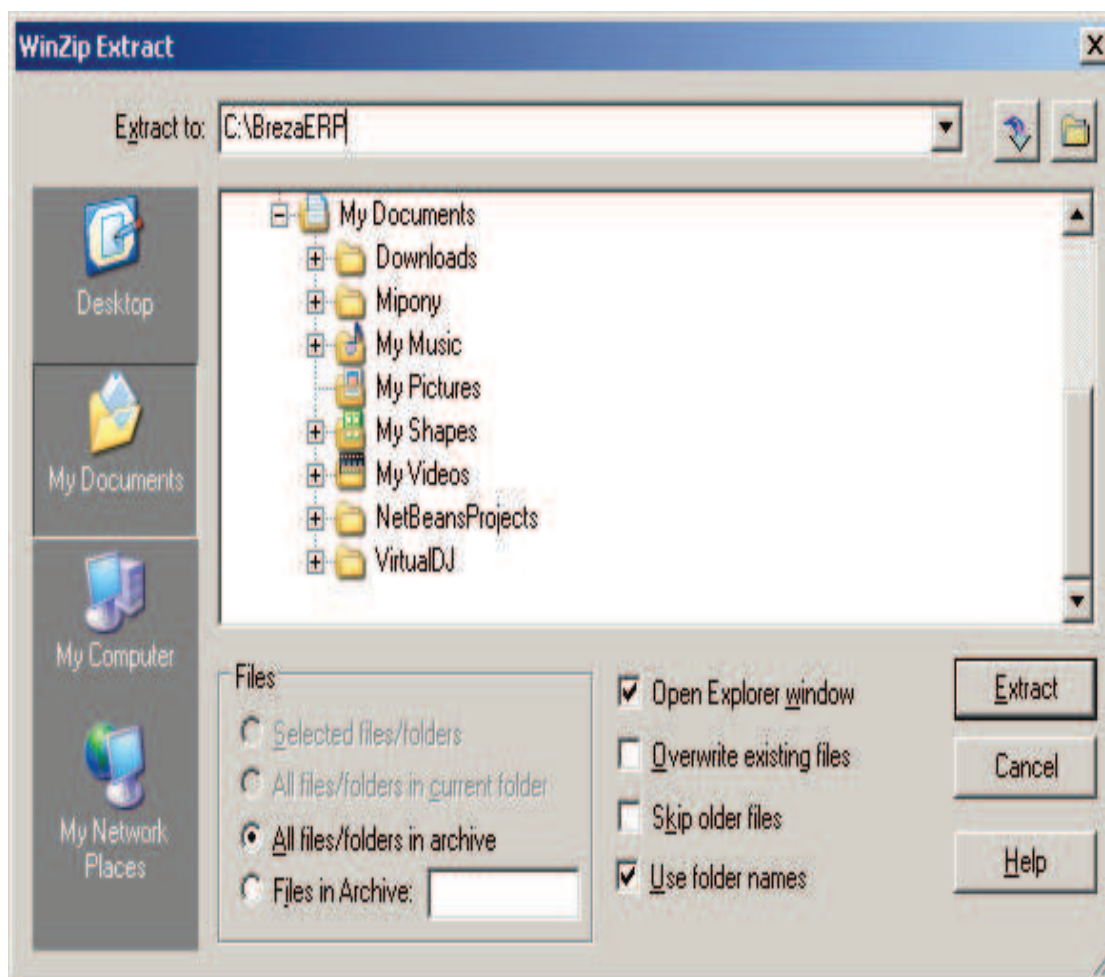
Слика 13: Снимање клијента на хард диск

После одабира места на ком ће се снимити SoftwareFull.zip потребно је из **My Computer** –а распаковати овај фајл на жељену дестинацију следећим поступком:

- 1) Десни клик на фајл -> WinZip-> Extract to... .
- 2) Изабрати дестинацију за инсталацију:

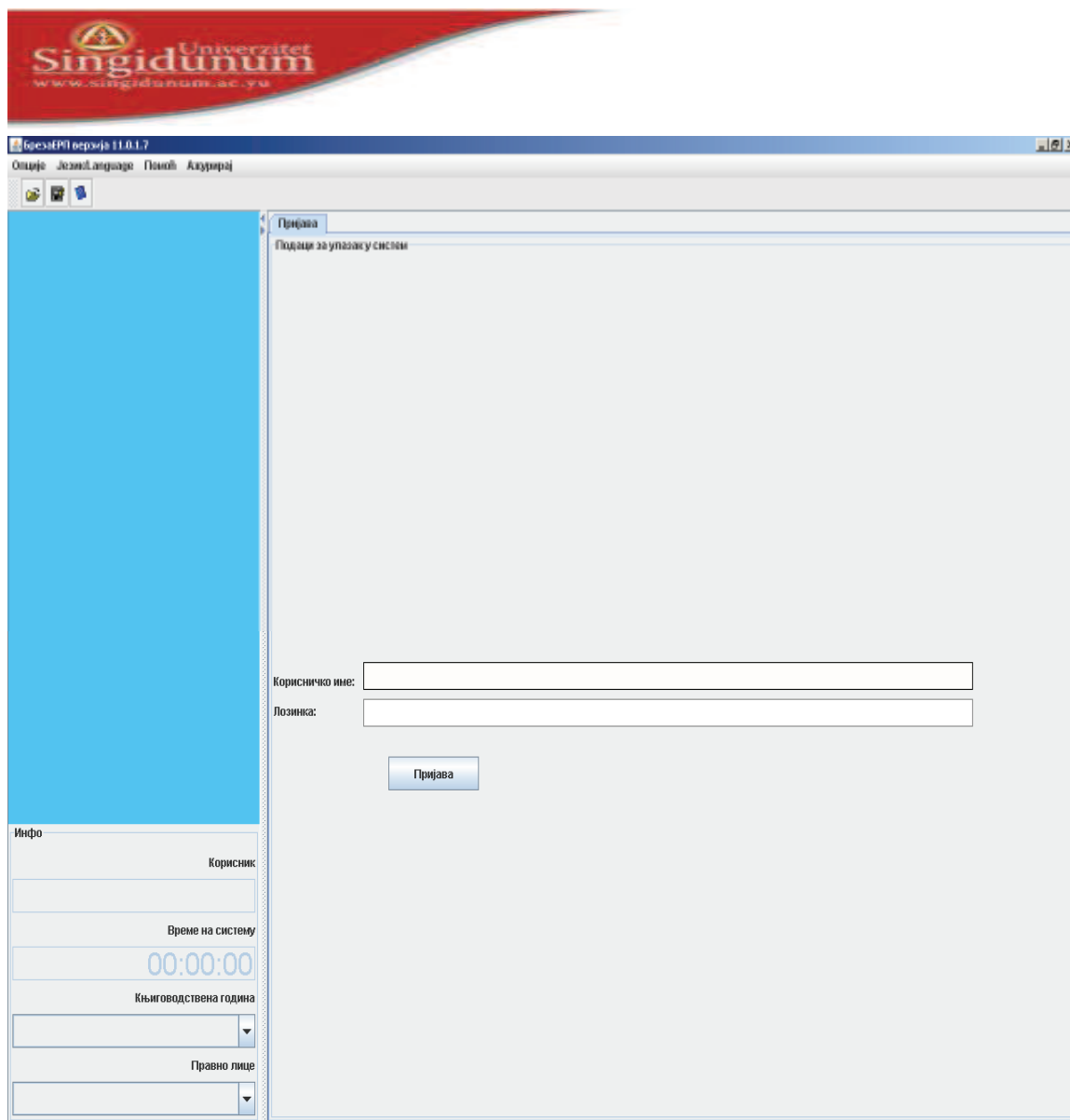
Одабир дестинације за распакивање фајла SoftwareFull.zip пример приказан на Слици 14. Сада кликнемо левим кликом на опцију Extract и добијамо клијент

инсталацију.



Слика 14: Одабир дестинације за распакивање фајла SoftwareFull.zip

Када смо распаковали фајл SoftwareFull.zip два пута кликнути на фајл **BrezaErp.bat** и добиће се почетни прозор апликације који је приказан на Слици 15.



Слика 15: Почетни прозор апликације

II ПОГЛАВЉЕ

4. Хардверске компоненте које су уграђене у информациони систем Дирекције за управљање одузетом имовином

4.1 Периферна опрема

У склопу имплементације пројекта информационог система Дирекције за управљање одузетом имовином испоручена је следећа прериферна опрема:

Ставка	Количина	Назив	Опис
1.	3	Лаптоп	FTS LIFEBOOK A531
2.	3	Мобилни штампач	Cannon PIXMA IP100
3.	3	Скенер великог капацитета	Cannon DR7750C +NW SCANNING DEVICE C660GB
4.	5	Мрежни штампач	Cannon LBP6300DN
5.	15	Радна станица	FTS ESPRIMO E500 E85+

4.2 Хардвер и системски софтвер

У склопу имплементације пројекта информационог система Дирекције за управљање одузетом имовином испоручен је следећи хардвер и системски софтвер:

Ставка	Количина	Назив	Опис
1.	3	Сервер	FTS PY RX300S6 8x2.5 gold PSU
2.	1	VMware лиценце за бекап сервер (VMware vSphere 4)	VMware vSphere 5 Essentials Plus Kit for 3 hosts
3.	1	Оперативни систем и софтвер за управљање базама података	Мајкрософт оперативни систем и софтвер за управљање базама података неопходним за подршку понуђеног решења
4.	1	Систем за чување података	FTS ETERNUS DX80 S2
5.	2	Концентратори локалне мреже	Mikrotik RB1100AH
6.	2	Заштитна баријера	Mikrotik RB1100AH
7.	1	19” серверски орман	FTS PRIMECENTER M1 Rack 742A 42U-1050x700

5. Техничке карактеристике хардверских компоненти:

5.1 Лаптоп -FTS LIFEBOOK A531

Приказ Мобилног рачунара који се користи за куцање записника кад се одузима имовина **Слика 16.**



Процесор - Intel® Core™ i5 2450M Processor 2.5GHz
Чипсет -Intel® HM65
Кеш меморија - 3MB
Hard DISK -SATA, 5400 rpm, 500 GB, 2.5-inch, S.M.A.R.T.
Мрежа - Ethernet
Wi-fi : Intel® Centrino® N1030 b/g/n
РАМ - 4 GB (1 module(s) 4GB) DDR3, 1333 MHz, PC3-10600, SO DIMM
Графичка картица - Intel® HD 3000
Дисплеј - 15.6" HD LED anti glare (1366 x 768)
Оптички уређај - DVD Super Multi
Интерфејс - USB 2.0 total - 3 (1 x Anytime USB Charge functionality)
VGA x1
HDMI x1
Ethernet (RJ-45) x1
DC-in x1
Аудио : line-in / microphone x1
Аудио : line-out / headphone x1
Читач картица - 4-in-1 card reader
ОС - Provided Microsoft® Windows 7® Professional 64-bit
Dimenzije - (WxDxH) 378 x 252 x 36.5 mm
Тежина - 2.5 kg
Батерија - Li-Ion battery 6-cell, 4400 mAh, 48 Wh - up to 7 h 20 min

5.2 Мобилни штампач-Cannon PIXMA IP100

Приказ Мобилног Штампача који се користи за штампање записника на терену
Слика 17.



Резолуција штампања - До 9600 x 2400 tpi
Механизам штампања - Инкџет штампач са пет боја мастила, микромлазницама минималне величине 1 pl i FINE главом за штампу
Брзина са квалитетом фотолабораторије - 10 x 15 cm, без маргина: приближно 50 секунди (стандардно)
Брзина штампања у црно-белој боји ESAT: приближно 9 слика у минути
Брзина штампања у боји ESAT: приближно 5,9 слика у минути
Конфигурација кертрица мастила Кертриц – PGI-35 Crni, CLI-36 Воја
Дужина трајања резервоара са црним мастилом Црно: 191 страница
Црно: 2080 фотографија
Дужина трајања резервоара са мастилом у боји Боја: 249 страница
Боја: 111 фотографија
Тип папира - Обичан папир, коверте, фото-папир Про (PR-101), сјајни фото-папир Плус (PP-101/PP-201), dvostrani foto-papir Plus (PP-101D), polusjajni foto-papir Plus (SG-201), sjajni foto-papir (GP-401), sjajni foto-papir za svakodnevno korišćenje (GP-501), mat foto-papir (MP-101), papir visoke rezolucije (HR-101N), papir za štampanje na pamuku (TR-301), foto-nalepnice (PS-101), super beli papir (SW-201)
Улаз папира - Механизам за увлачење листова: макс. 50 листова
Величина папира - Механизам за повлачење листова: A4, B5, A5, Letter, Legal, коверте (величине DL ili Commercial 10), 10 x 15 cm, 13 x 18 cm, 10 x 18 cm (широко), 20 x 25 cm, кредитна картица (54 x 86 mm)
Тежина папира - Механизам за повлачење листова: 64 до 105 g/m ² и подршка за Canon специјалне медије до 273 g/m ²
Двострано штампање - Ручно управљање могуће је када се користе двострани фото-папир Плус, супер бели папир или обичан папир формата A4, B5, A5, Letter i 13 x 18 cm (samo Windows)

5.3 Скенер великог капацитета **Cannon DR7750C**

Скенири за врло брзо скенирање докумената, користи се за пребацивање свих докумената из папирне форме у електронсуј форму **Слика 18.**



Тип - Стони скенер с улагачем листова
Сензор јединице за скенирање - 3-linijski CMOS CIS сензор
Оптичка разлучивост - 600 dpi
Страна за скенирање - Предња/стражња/обострано
Брзина скенирања - Црно-бело/ сиве нијансе: 200/300 dpi: 75 ppm / 150 ipm (Портретно A4); 90 ppm / 180 ipm (Пејзажно A4)
У боји: 300 dpi: 75 ppm / 150 ipm (Портретно A4); 90 ppm / 170 ipm (Пејзажно A4)
Напајање - AC 220 - 240 V (50/60 Hz)
Потрошња енергије Скенирање: 84 W, стање мировања: 3,9 W (AC 220-240 V), напајање искључено: 0 W
Радно окружење - 10 - 32,5 °C, влажност: 20 - 80% RV
Ширина - 50,8 - 305 mm
Дужина - 70 - 432 mm
Automatic Feeding Начини улагања - аутоматски, континуирано ручно и увлачење из ручног улагача Улагање с помаком уз могућност блокирања бочних водилица
Long Document Mode 3000 mm maks. (могуће постављање на управљачкој плочи)
Gramatura Аутоматско улагање: 52 - 209 g/m2 (0,06 - 0,25 mm)
Ручно улагање: 40 - 255 g/m2 (0,05 - 0,30 mm)
Rad s dugim dokumentima 3000 mm maks. (могуће постављање на управљачкој плочи)
Одвајање папира - Успорни ваљак
Капацитет улагача 500 листова
Moguć odabir 500, 300, 100 listova
Разлучивост 100 x 100 dpi, 150 x 150 dpi, 200 x 200 dpi, 240 x 240 dpi, 300 x 300 dpi, 400 x 400 dpi, 600 x 600 dpi

5.4 Мрежни штампач Cannon LBP6300DN

Овај штампач се користи за разне врсте штампе углавном преко њега се врши штампање великих броја страна као што су закони, систематизације и други документи из делукруга рада дирекције за управљање одузетом имовином **Слика 19.**



Брзина штампе - 30 страница у минути за црно-бело штампање (A4)
Методе штампе - Монохроматска ласерска штампа
Квалитет штампе - До 2400 x 600 dpi са аутоматским побољшавањем слике
Резолуција штампе - До 600 x 600 dpi
Време пуњења - Приближно 10 секунди или мање од укључивања
Прва страница - Приближно 6 секунди или мање
Циклус Штампе - Макс. 25.000 страница месечно
Улазни папир - (Стандард) Касета за 250 листова
Типови папира - Обичан папир, тежак папир, паус, налепница, картица са индексом
Величина - Касета (стандардно и опционално): A4, B5, A5, A6, Legal, Letter, Executive, 16K, Prilagođene dimenzije: širina 105 mm do 215,9 mm; dužina 148,0 mm do 355,6 mm.
Вишенаменско лежиште: A4, B5, A5, A6, Legal, Letter, Executive, 16K, koverta DL, koverta COM10, koverta C5, koverta Monarch, kartica sa indeksom 76,2 mm do 127 mm, prilagođene veličine: širina 76,2 do 215,9 mm; dužina 127,0 do 355,6 mm.
Тежина папира Касета (стандардна и опциона): 60 до 120 г/м²
Вишенаменско лежиште: 60 до 163 г/м²
Обострана штампа - Аутоматско
Повезивање - Brza USB 2.0 veza 10Base-T/100Base-TX
Подржани ОС - Windows 2000/ Server 2003/ Server 2008/ XP/ Vista/ 7

Mac OS X verzija 10.4.9-10.6 Linux
Димензије - (W x Д x X) 400 мм x 376 мм x 260 мм
Тежина - Приближно 11,8 кг

5.5 Радна станица FTS ESPRIMO E500 E85+

Ова радна станица користи се за унос предмета у електронску форму као и за остале канцеларијске послове **Слика 20.**



Процесор - Intel Core i3-2120
Чипсет - Intel® B65
Такт процесора - 3 MB, 3.30 GHz
Меморија - 4GB
Капацитет хард диска - 500GB
Брзина ротације хард диска - 7200rpm
Оптички уређај - DVD SuperMulti SATA
Дијагонала монитора - 19"
Тастатура и миш - Keyboard KB400 USB black SEE Optical USB wheel mouse
Графичка картица - Intel HD
Повезивање - 1 x Audio: line-in, 1 x Audio: line-in / microphone, 1 x Audio: line-out 1 x Front audio: headphone, 1 x Front audio: microphone 1 (DVI-D) x DVI, 1 (optional) x eSATA, optional x USB 3.0 total, 10 x USB 2.0 total, 2 x USB front, 6 x USB rear, 2 x USB internal 1 x Ethernet (RJ-45), 1 (optional) x Parallel (25pin) 2 x Mouse / Keyboard (PS/2), 1 x Serial (RS-232) (9pin, 16 byte FIFO, 16550 compatible), 1 x VGA

Мрежа ЛАН: 10/100/1000 MBit/s Realtek RTL 8111E
--

Оперативни систем - Win7 Pro64 SEE+Office2010s

Остало - 280 W power supply, Audio: Realtek ALC663

Нето/Бруто маса - 10 kg

Димензије - 340 x 382 x 98 mm

5.6 Сервер FTS PY RX300S6 8x2.5 gold PSU

Заокружен црвеном бојом је један од укупно 3 сервера колико их тренутно има.
Главна функција сервера је обрада података и комуницирање са скаладиштем података **Слика 21.**



Процесор и чипсет
Type Intel Xeon E5620 / 2.4 GHz
Number of Cores -Quad-Core
64-bit Computing
CPU- Qty 1.0
Max CPU Qty 2.0
L2 cache 4 x 256 KB
CPU Upgradability Upgradable
Chipset Type Intel 5520

Кеш меморија
Installed Size L3 cache - 12.0 MB
Cache Per Processor 12 MB

РАМ
Installed Size 4.0 GB / 192.0 GB (max)
Technology DDR3 SDRAM - Advanced ECC
Memory Speed 1066.0 MHz
Memory Specification Compliance PC3-10600
Features Hot-swappable,
Triple channel memory architecture,
Registered,
Memory Mirroring
Configuration Features 1 x 4 GB

Оптички уређаји
Type DVD±RW (±R DL) / DVD-RAM - Serial ATA
Read Speed 24x (CD) / 8x (DVD)
Write Speed 24x (CD)
Rewrite Speed 16x (CD) / 6x (DVD-RW) / 8x (DVD+RW) / 5x (DVD-RAM)

Повезивање

Type Integrated
Ethernet Ports 2 x Gigabit Ethernet
Ethernet Controller Intel 82575EB
Data Link Protocol Fast Ethernet,
Ethernet,
Gigabit Ethernet
Remote Management Protocol IPMI 2.0
Remote Management Controller Integrated Remote Management Controller (iRMC S2)

Оперативни систем

Windows Server Certified Windows Server 2008 R2 Certified

Димензије

Width 19.0 in
Depth 30.3 in
Height 3.4 in
Weight 55.1 lbs

Складишни Controller

Type 1.0 x RAID - Plug-in card - PCI Express x4
Controller Interface Type Serial Attached SCSI 2
Storage Controller Name LSISAS2108
Channel Qty 8.0
RAID Level RAID 0,
RAID 5,
RAID 50,
RAID 1,
RAID 60,
RAID 6,
RAID 10
Buffer Size 512.0 MB

Хард диск

2 x 147 gb SAS

5.7 Систем за чување података FTS ETERNUS DX80 S2

Место где се складиште сви подаци из информационог система **Слика 22.**



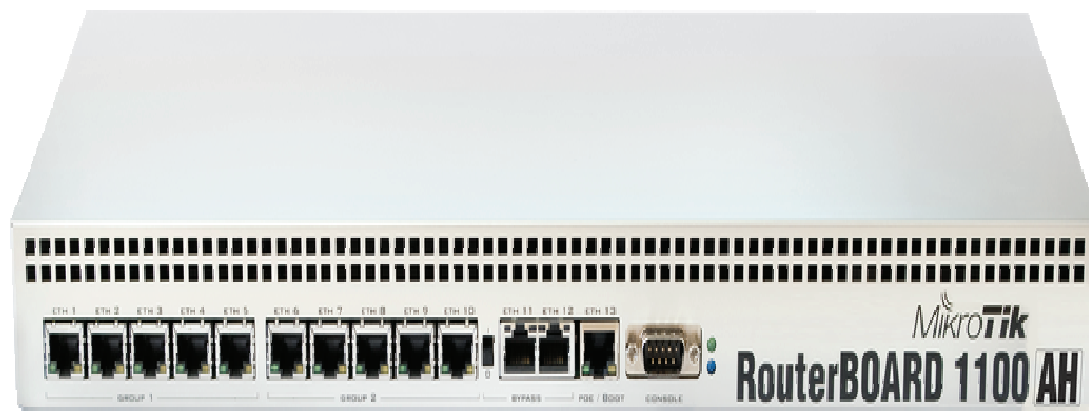
Хард диск
Укупни простор за податке - 2000 GB
Број подржаних хард дискова - 120
Капацитет хард диска - 1000 GB
Брзина обртаја хард диска - 7200 RPM
Максимални капацитет - 240 TB
RAID varijante - 0, 1, 1+0, 5, 5+0, 6
Interfejs hard diska - Serial Attached SCSI (SAS)
Величина хард диска - 64 mm (2.5 ")
Podržani HDD interfejsi - SAS
Мрежа
Сагласност са индустријским стандардима - IEEE 802.3, IEEE 802.3u
Технологија каблирања - 10/100Base-T(X)
Максимална брзина преноса података - 100 Mbit/s
Повезивање
Broj Ethernet LAN (RJ-45) portova - 1
RS-232 port -1
Платформа за управљање - Web, CLI
Протоколи за управљање - SNMP
Веб-басед управљање - Da
Дугме/прекидач за укључивање и искључивање - Da
Технички детаљи
Тип кућишта - Rack (2U)
ЛЕД индикатори - Da

Менаџмент потрошње
Потрошња енергије - 630 W
Број напајања - 1
Тежина и димензије
Тежина - 35 kg
Радни услови
Радни опсег влажности - 20 - 80 %
Распон радне температуре (Т-Т) - 10 - 40 °C
Дозвољена надморска висина - 0 - 3000 m
Тежина - 35 kg

Потрошња струје - 100 - 240 V, 50 - 60 Hz
Компатибилни оперативни системи
Windows Server 2008 Standard (32/64-bit)
Windows Server 2008 R2 Standard (32/64-bit)
Windows Server 2008 Enterprise (32/64-bit)
Windows Server 2008 R2 Enterprise (32/64-bit)
Windows Server 2008 Datacenter (32/64-bit)
Windows Server 2008 R2 Datacenter (32/64-bit)
Windows 7 Home Premium
Windows 7 Professional
Windows 7 Ultimate
Windows Vista Home Basic
Windows Vista Home Premium
Windows Vista Business
Windows Vista Enterprise
Windows Vista Ultimate
Windows XP Home Edition
Windows XP Professional
Могућности мреже - Fast Ethernet
Power ЛЕД - Da
ЛЕД показивачи конекције - Da
конекција/активација ЛЕД сигнализација - Da
Брзина преноса података - 8 Gbit/s

5.8 Концентратори локалне мреже Mikrotik RB1100AH

Уређај који у овом информационом систему врши комуникацију између сервера и складишта података **Слика 23.**



CPU speed - 1066MHz
RAM - 2GB
Архитектура - PPC
LAN port - 13
Gigabit - Da
MiniPCI - 0
Integrated Wireless - 0
USB - 0
Меморијска картица - 1
Меморијска картица тип - microSD
Прикључак за напајање - 110/220V
802.3af support - Ne
PoE - 12-24VDC
Voltage Monitor - Da
CPU температура монитор - Da
Димензије 1U case: 44 x 176 x 442 mm, 1200g. Board only: 365g
Оперативни систем – Router OS
Опсег температуре -25°C to +65°C
RouterOS License - Level6
CPU - P2010
Максимална потрошња - 20W

**5.9 19" серверски орман FTS PRIMECENTER M1 Rack 742A 42U-
1050x700**

Серверски ормар у који се смештају Сервери, складишта података, концентратори мрежа, приказан је на **Слици 24.**



Тежина и величина
Ширина - 700 mm
Дубина - 1050 mm
Висина - 2003 mm
Тежина - 122 kg
Максимална тежина (capacity) 1000 kg
Величина - (WxDxH) 800 x 1200 x 2150 mm
Боја
Боја производа црна
Оперативни опсег влажности - 15 - 98 %
Сертификати
Certification GS
CE
EN
FCC Class A
UL/CSA
CB
RoHS
WEEE
Технички детаљи
Место у ормару - 42U
Тип - Freestanding

Поглавље III

6. Заштита информационог система Дирекције за управљање одузетом имовином

6.1 ЕЛЕКТОНСКО ПОСЛОВАЊЕ И БЕЗБЕДНОСТ ИНФОРМАЦИОНИХ СИСТЕМА

Електронско пословање је општи концепт који обухвата све облике пословних трансакција или размене информација које се изводе коришћењем информационих и комуникационих технологија [16]. Са аспекта комуникација електронско пословање је електронска испорука информација, производа и услуга коришћењем рачунарских мрежа. Са пословног аспекта то је примена технологије у сврху аутоматизације пословних трансакција и пословања уопште. Са становишта услуга то је алат који омогућује смањење трошкова пословања уз истовремено повећање квалитета и брзине пружања услуга. Електронско пословање заснива се на примени Интернета, Интранета и апликација за групни рад. Предности електронског пословања произилазе из комбинације економских и технолошких разлога. Међу економским разлозима су:

- **смањење трошкова пословања,**
- **смањење грешака код електронских трансакција,**
- **јефтино глобално публикување трансакција,**
- **могућност замене скувих канцеларија.**

Електронско пословање омогућава унутрашњу и спољну интеграцију предузећа. Највећи проблем је питање безбедности рада тј. заштита података од неовлашћеног приступа и промена, и заштита кредитних картица приликом куповине преко мреже и сл. То је проблем који захтева веће техничке и организационе иновације, како би се у што већој мери спречиле злоупотребе. Потребно је решити и питање заштите ауторских права, заштите приватности појединаца и заштита од компјутерских вируса. Да би се електронско пословање могло развијати, потребно је испунити неке технолошке претпоставке. Осим технолошких претпоставки потребно је остварити и законске претпоставке које ће омогућити несметан развој електронског пословања

Разлози за оптимистичка предвиђања брзог развоја електронског пословања су:

- **изванредно брз технолошки развој,**
- **развој нових сервиса и пословних модела,**
- **развој националних и међународних стандарда и водича за електронско пословање.**

6.2 БЕЗБЕДНОСТ

Безбедност информација је важна у савременом друштву. Државни субјекти све више су зависни од ИКТ инфраструктуре. Кроз њу се врши проток велике количине информација између субјеката унутар система, али једно излаже информације и информационе системе ројним претњама. Појам безбедности информација не дноси се искључиво на техничке мере заштите логовање, криптовање), него и административне (сигурносне политике, правилнике, процедуре) као и физичке (физичка контрола приступа, видео надзор, итд.). За успостављање безбедности информационих система усвојен је међународни стандард система менаџмента за безбедност информација ISO 27001 Standard ISO 27001 је конципиран у пет поглавља и то: Систем за управљање безбедношћу информација (ISMS), Одговорност руководства, Интерна провера ISMS, Преиспитивање ISMS од стране руководства и Унапређење ISMS. Приликом успостављања стандарда ISO 27001 установљена је компатибилности са стандардом ISO 9001 и јасно је истакнут модел стандарда кроз PDCA (Plan-Do-Check-Action/planirajizvrši- proverideluj) циклус сталног унапређења. Поступци за планирање, спровођење, мерење и побољшање процеса представљају основне задатке модерног безбедоносног система. То значи да сваку активност треба планирати, реализовати, па потом проверити и на основу тог искуства предузети мере за побољшање. PDCA циклус (слика 25.) симболизује затворену петљу редоследа извођења укупног посла и појединачних пословних процеса у моделу процеса безбедности правосудног информационог система. PDCA методологија може се, укратко,

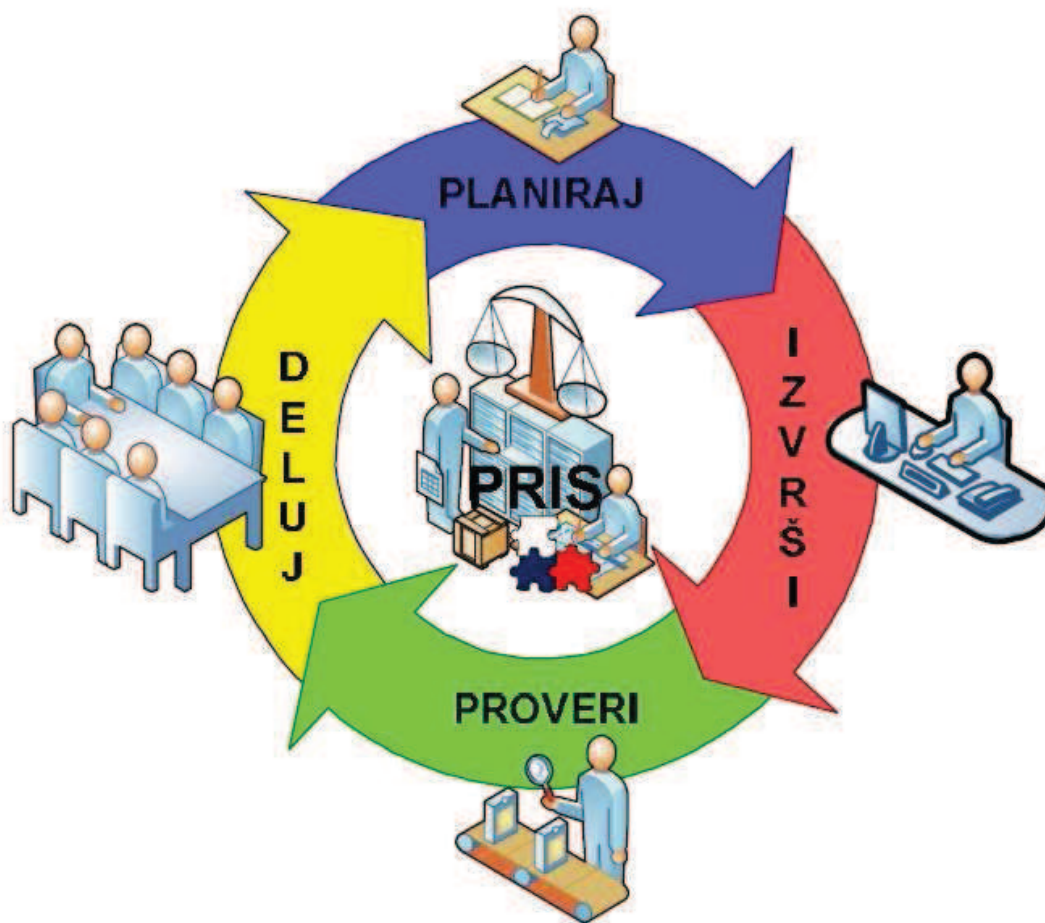
описати на следећи начин:

- **Планирај:** утврди циљеве и процесе потребне за добијање резултата. На основу исказаних захтева корисника и кроз успостављање политике ИСМС организација, врши се планирање система ПРИС за управљање безбедношћу информација. У овој фази се спроводе и активности на дефинисању критеријума и методологија за оцену ризика.

- **Изврши:** примени процесе. У овој фази се спроводи планиран и примењује се претходно дефинисан управљачки механизам и дефинишу структура и одговорности, обука, компетентност и свест, документација и контрола докумената, контрола над операцијама и спремност на реаговање у ванредним ситуацијама.

- **Провери:** прати, мери процесе и извештавај о резултатима. На основу дефинисаних процедура за преиспитивање, мерење ефективности управљачких механизма, спровођења интерних провера, ажурирање планова за снижавање ризика и др врше се праћења и мерења, вредновања усаглашености, корективних и превентивних акција, управљања записима и интерних провера система.

- **Делуј:** предузимај све мере за стално унапређење система. Преиспитивање од стране руководства које заокружује цео циклус перформанси система менаџмента и враћа га на планирање које треба да резултује стално побољшање преузимањем корективних корака и дефинисању превентивних мера, провера дали су спроведена побољшавања одржива.



Слика 25. Модел система менаџмента за безбедност информација заснован на PDCA циклусу

Стандарда ISO / IEC 27001 захтева систематско испитивање ризика организације информационе безбедности, узимајући у обзир претње, рањивости и утицај. Такође захтева да се осмисли и спроведе кохерентан и свеобухватан пакет контрола информационе безбедности и / или друге облике ризика третмана (као што су избегавање ризика или ризика преноса) на оне ризике који се сматрају неприхватљивим и Усвојити свеобухватни процес управљања како би се осигурало да информације безбедносне контроле и даље задовољавају информационе безбедности организације. Ово установити као стални процес. Стандарду ISO / IEC 27001:2005 је намењен да буде погодан за више различитих типова употребе,

укључујући следеће:

- користе у организацијама да формулишу захтеве у погледу заштите и циљева;
- коришћење у оквиру организације као начин да се осигура да се безбедносним ризицима ефикасно управља;
- користе у организацијама да обезбеде усклађеност са законима и прописима;
- коришћење у оквиру организације као процесни оквир за имплементацију и управљање контроле како би се осигурало да се испуне одређени безбедносни циљеви организације;
- дефинисање нових информационих процеса безбедности за управљање;
- идентификацију и разјашњавање постојећих информационих процеса безбедности за управљање;
- коришћење од стране менаџмента организације да одреди статус активности информисања о безбедности за управљање;
- коришћење од стране интерних и екстерних ревизора организација да се утврди степен усклађености са смерницама, директивама и стандардима усвојеним од стране организације;
- коришћење од стране организације да пружи релевантне информације о политици информационе безбедности, директивама, стандардима и процедурама другим организацијама са којима сарађује из оперативних разлога;
- имплементација сигурности информација;
- коришћење од стране организације у циљу пружања релевантних информација о безбедности информација за клијенте.

У оквиру ISO 27000 стандарда постоји део ISO / IEC 27036 - IT - Смернице за безбедност аутсорсинга. JUS ISO / IEC 27036 води рачуна о проценама безбедносних ризика који су укључени у набавку и коришћење спољне услуге, подршку имплементацији ISO / IEC 27002 за безбедност контроле везане за outsourcing. Покривене су следеће широке области:

Стратешки циљеви, циљеви и пословне потребе [у односу на безбедност информација];

Информације о безбедносним ризицима и техникама;

Обезбеђење квалитета (у складу са уговорним обавезама, итд.)

Односи се на "outsourcing" животног циклуса "и то: Иницијација - одређивање оквира, Business Case / costbenefit анализа, поређење инсоурце насупрот outsource опције, као и варијанта приступа, као што су cosourcing; Дефинисање оутсорсинг захтева, укључујући захтеве сигурности информација; Набавке, укључујући процену и уговарање са пружаоцима услуга (важно је да се опште одговорности и одговорности за безбедност изричито договоре у овој фази);

Транзиција или имплементација оутсоурсинг аранжмана;

Експлоатација укључујући и аспекте као што су

релационски манаџмент, комплијансе, инцидент и

управљање променама, итд;

Унапређење (опционо у фази обнове уговора);

Окончање односно понављање ка оутсоурсу или

враћање у insourcing.

"Outsourcing" у овом контексту није ограничено на ИКТ outsourcing већ обухвата и друге облике, као што су измештање људских ресурса, управљање објектима и другим пословним процесима који имају информације безбедносне импликације. Outsourcing i backoffice пословање очигледно повећава зависност организације ка спољним провајдерима - пружаоцима услуга у домену ИКТ и ствара окружење "продуженог поверења". Тиме се „дели” одговорност за безбедност информација. Outsourcing аранжман такође треба да узме у обзир нове или измене постојећих захтева у домену сигурности информација, на пример оне које намеће законодавна регулатива. JUS ISO / IEC 27002:2005 Сигурносне технике - Кодекс за информације Security Management, Члан 11: Контрола приступа. Логички приступ ИТ система, мрежа и података мора бити одговарајуће контролисана ради спречавања неовлашћеног коришћења. Овај члан има 7 тачака које дефинишу процедуралне и практичне захтеве у домену сигурности. Примена ISO стандарда није и не треба да буде јединина водиља у успостављању сигурности информациоог система. Потребно је пратити и препоруке Европске уније и њених тела која се баве овом проблематиком. Показало се веома корисно и практично праћење препорука Европске агенције за мреже и информационе системе - European Network and Information Security

Agency (ENISA), <http://www.enisa.europa.eu/>.

Postoje i jasne veze između ISO 27001 и препоруке

OECD-а о безбједности информација, смернице 2002 и документа Базелског комитета

"Добра пракса за управљање и надзор над оперативним ризиком." У Сједињеним Државама, регулаторни услови које, на пример, GLBA Закон (Gramm-Leach-Bliley Act), Здравствено осигурање преносивости и доступност закона (Хеалтх Инсуранце Портабилити анд Аваилабилити Act - HIPAA), the Californian Senate Bill 1386 i Online Personal Protection Act, naravno, kao SOKS (Sarbanes-Oxley Act - SOKS) и Савезни Закон о безбедности информација за управљање, је најбоље спознао преко развоја информационог система управљања сигурношћу која је интегрисана, свеобухватно у ISO 27001 стандарду.

6.3 СТАНДАРДИ

SRPS ISO/IEC 27001 (Информационе технологије - Технике безбедности - Системи менаџмента безбедношћу информација - Захтеви) је национални стандард који је настао као резултат потребе дефинисања међународно прихваћених норми, који ће својим захтевима дефинисати оквир формирања свеобухватног система заштите и циљеве његовог деловања како би се на ефективан и ефикасан начин управљало безбедношћу информација [18]. Овај стандард је идентичан стандарду ISO/IEC 27001 и спецификује захтеве за успостављање, имплементацију, примену, праћење, преиспитивање, одржавање и побољшавање документованог ISMS унутар контекста укупних пословних ризика у организацији; спецификује захтеве за имплементацију безбедносног управљања прилагођеног потребама појединих организација или њихових делова.

Стандард ISO 27001 је конципиран у пет поглавља и то: .

Систем за управљање

безбедношћу информација (ИСМС), Одговорност

руководства, Интерна провера ИСМС, Преиспитивање ИСМС од стране руководства и Унапређење ИСМС. ИСО 27001 је мултидисциплинаран, јер третира безбедности информација са три аспекта:

- **Информационог** – анализирајући и дефинишући перформансе

ИТ опреме, права приступа, криптовања, лозинке, протоколе, политике са аспекта појаве ризика по безбедност података и информација

- **Административног** – дефинишући јасна упутства, политике и процедуре за

генерисање информација, њихову дистрибуцију, чување (складиштење)

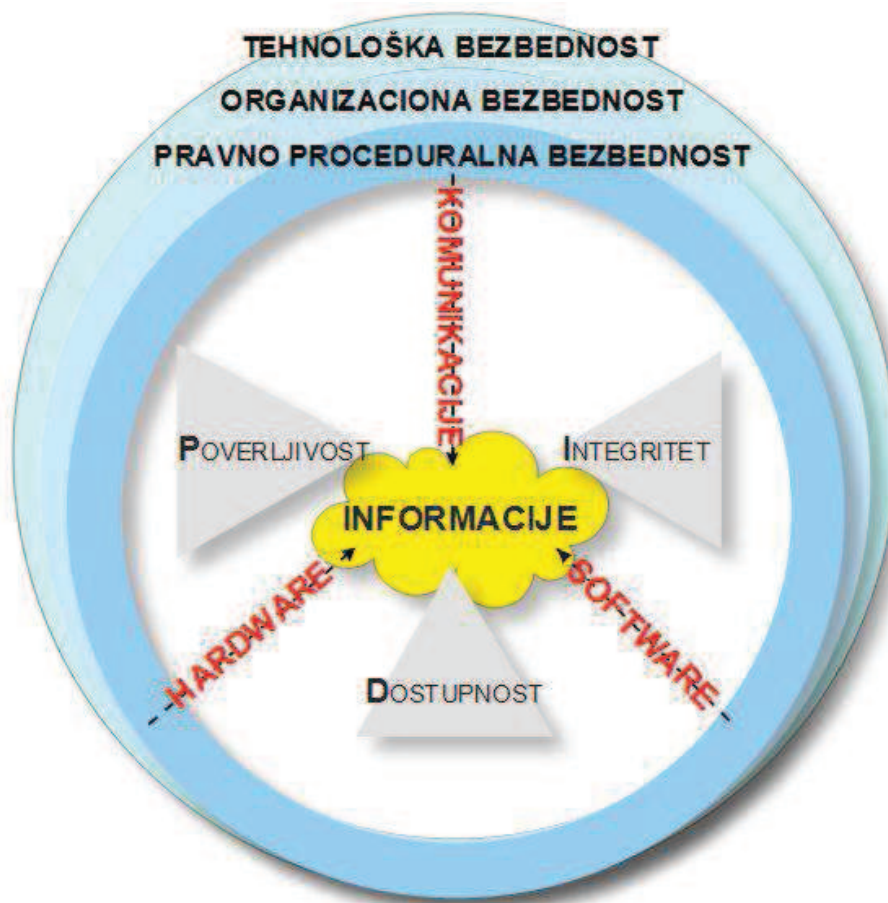
- **Физичког** – физичка контрола приступа, евиденција запослених, видео надзор, заштита радних просторија. Предности које имплементација и сертификација ISO 27001 носи са собом, могу се сажети у два сегмента. Први сегмент је заштита и безбедност информација кроз систематски и проактиван приступ за идентификовање и деловање против читавог низа потенцијалних ризика којима су изложене информације организације. Управљајући ризиком по безбедност информација, умањује се вероватноћа појаве непредвиђених ситуација. Компоненте Безбедности информација:

Поверљивост

(Confidentiality), **Интегритет** (Integrity) и **Доступност** (Availability) - PID (CIA). Информациони системи у том смислу групишу се у три целине: хардвер, софтвер и комуникације са циљем да се идентификују и примене стандарди безбедности информација, као и механизми заштите и превенције на три нивоа или слоја:

правно процедурални, организациони И технолошки (Слика 26.). У

суштини, процедуре или правила се спроводе да кажу службеницима (администратору, кориснику и оператеру) како да користе ИКТ како би се осигурала безбедност информација у оквиру Правосудног информационог система. Стандард SRPS ISO 27001 је ступањем на снагу Уредбе о посебним мерама заштите тајних података у информационо - телекомуникационим системима („Службени гласник РС“, број 53/2011 од 20. јула 2011. године) од препоруке постао правно процедурални оквир и неизоставни чинилац свих информационих система државе Србије. Чланом 10 ове уредбе препознат је национални стандард SRPS ISO/IEC 27001 у складу са којим ће се спроводити заштита тајних података у информационо – телекомуникационим системима.



Слика 26. Компоненте безбедности информација

Добити од имплементације Система менаџмента безбедности информација (ISMS), сагласно захтевима ISO 27001:2005, у Правосудни информациони систем могу бити следећи:

- ”Just in time” ефекат – Права информација на право место у право време,
- Заштита и очување know-how,
- Повећање ефективности и ефикасности система,
- Повећање пословног кредибилитета и поверења од стране клијената и партнера,
- Уштеда времена рационализацијом количине и садржине информација,
- Оптимизација ресурса потребних за дистрибуцију и чување података,
- Рана идентификација рањивости, претњи и потенцијалних

негативних утицаја на пословање,

- Смањење ризика од запошљавања људи који би могли нашкодити систему,
- Постизање синергетског ефекта тимског рада,
- Промптна усклађеност са законском регулативом,
- Бржи проток информација између запослених,
- Стварање предуслова за одређивање одговорности,
- Смањење неспоразума код запослених услед "укрштања информација",

Значајне су користи које модел за уређење система за безбедност информација ISO 27001 остварује организацијама које се одлуче да га имплементирају, пре свега у смислу побољшавања својих организационих перформанси. Извесно је да овај модел представља најбољу праксу у области заштите и безбедности информација која је преточена у захтеве стандарда.

6.4 ЗАШТИТА СИСТЕМА У ПРАВОСУЂУ

Сигурност рачунарских система постаје све важнија, јер све више корисника на све више начина користи све више информација у рачунарском свету [19]. У таквом систему постоји и све већа опасност од неовлашћене употребе информација, подметања погрешних информација или уништавања информација.

У рачунарским системима информације се преносе разноврсним отвореним и несигурним комуникацијским путевима. Приступ до тих путева не може се физички заштитити па сваки непријатељски настројен нападач може нарушити сигурност система. Због тога заштитни комуникацијски механизми над несигурним комуникацијским каналом постају најважнији облик остварења сигурности. Показује се да једна од најделотворнијих заштита порука њихово криптовање. Обезбеђење заштите података једно је од најзначајнијих и најделикатнијих питања са којима се сусрећу сва демократска друштва и информациони системи у њима.

Правосудни информациони системи посебно су значајни, јер је потреба за разменом података унутар правосуђа огромна, као и могућност њихове злоупотребе. Да би се онемогућила злоупотреба и обезбедила заштита података предузимају се одређене правне, техничке, организационе и друге посебне мере државе. Иако последње на листи, међу најважније спадају посебне мере државе којима се штити држава од

злоупотребе нарочито поверљивих података, али и целокупни национални спектар информационих система. Оне се реализују правилним конципирањем укупне политике информационе делатности, затим политике функционисања и развоја "јавних" база података, као и политике заштите података у интерним и екстерним токовима државе. Правним мерама се кроз правну регулативу, законе, подзаконске акте, дефинишу начини заштите података и процеси везаних за те податке. Овим мерама се дефинише и инфраструктура којом се крећу подаци, као и поступање са подацима, нпр. начин прављења резервних копија, софтверска документација, документација о рачунарским мрежама и сл. Овим мерама се ближе дефинише оквир поступања са подацима, нпр. у делу заштите података о личности и то поштовањем одређених принципа који су законом успостављени. Овде свакако спадају и одредбе Судског пословника као и Пословника о раду јавних тужилаштава. Теничке мере морају да обезбеде функционалност Правосудног информационог система уз потпуно уважавање правно процедуралне материје али и сагледавања тог система у реалном техникотехнолошком окружењу. Све техничке мере морају се дефинисати у техничкој документацији, за сваки појединачни део посебно. Техничке мере подразумевају директне мере за техничке системе и подсистеме, али и индиректне инфраструктурне системе подршке раду на којима се базира потпуно функционисање Правосудног информационог система као техничког система.

Организационе мере дефинишу накритичнији део заштите *informacionih sistema* – ИКТ

особље унутар система. То подразумева оснивање такве организације која ће се бавити развојним, стручним и регулаторним пословима од интереса за правосуђе и грађане, а поготово што ови послови не захтевају сталан и непосредан политички надзор и што таква организација може боље и делотворније да их врши него орган државне управе или правосудни орган. Значајно је и то да се у целини или претежно Правосудни информациони систем, заједно са свим јавним регистрима у њему (судски тумачи, вештаци, извршитељи, медијатори, бележници), може делимично финансирати од цене коју плаћају корисници услуга, односно грађани, предузећа, адвокати, инвеститори и др. Оваквом организацијом обезбедили би се стручни и мотивисани службеници, адекватно информатички образовани, а не приучени или „обучени“, и уједно дисциплиновани да спроводе послове заштите података. Изазвано недавним догађајима, у пракси познато већ дуже време, намеће се неопходност успостављања

радног места ИТ администратора за безбедност података (Дата Сецуриту Администратор) који не би били подређени руководиоцу правосудног органа у коме раде, већ директно руководиоцу безбедности *Pravosudnog informacionog sistema* (Chief Security Officer) како би свој посао обављали несметано у складу са правилима струке. Заштита података представља скуп метода и техника којима се ограничава приступ подацима од стране програма који се извршавају, или у једном ширем смислу заштита подразумева скуп метода, техника и правних норми којима се ограничава приступ подацима од стране програма и људи. Путем заштите штити се физички интегритет целокупног информационог система, било да је дистрибуиран или не, односно централизован или децентрализован. Децентрализовани информациони системи су посебно сложени за спровођење послова безбедности. Заштита података обухвата скуп међусобно повезаних активности, метода, техника и норми којима се обезбеђује приватност, сигурност, поверљивост, расположивост и интегритет података од свих опасности које им прете. Активности, методе, технике и норме морају бити дефинисане усвојеним стандардима и *ICT Security Policy* документима које ће ИКТ експерти примењивати и стриктно их се придржавати у свакодневном раду са корисницима система. Сигурност података обухвата заштиту података од откривања неовлашћеним корисницима, или неовлашћеног ажурирања овлашћеним корисницима. Наиме, сигурност претпоставља да су корисницима доступни само они подаци који то могу и треба да буду. Поверљивост произилази из својинских односа и значаја података за одређене субјекте. Поверљиви подаци се не смеју открити од стране неауторизованих појединаца или других ентитета, а такође ни у неовлашћеним процесима. Расположивост подразумева могућност овлашћеног корисника да благовремено дође до одређених података. Интегритет података претпоставља да се подаци не смеју неауторизовано ажурирати.

6.5 БЕЗБЕДНОСТ КАО СТРАТЕШКО ОПРЕДЕЉЕЊЕ

У информационом друштву се као нежељени ефекат појављује угрожавање информационе безбедности. Информациона безбедност је процес сталног одржавања сигурности корисника и информационог система. Стратешко опредељење српског правосудја свакако мора бити безбедност Правосудног информационог система. Главни задаци стратегије морају бити:

- **Превенција** – Превентивно деловање је најефикасније, али је и најскупље, јер захтава стално праћење трендова у појединачним доменима заштите. Овакав модел захтева већу кадровску јединицу.

- **Детекција** – Када дође до детектовња проблема боље је да та детекција буде рана детекција, јер олакшава одбрану од напада, са деловањима у циљу што мањег наношења штете.

- **Ограничавање штете** – Минимизовати и ограничити штету када се неисправност појави. Потребно је развити методе за контролу штете у поједним сегментима ИКТ система..

- **Опоровак** – ИКТ систем пројектовати на начин да се, из стања у отказу у потпуно функционално стање, оштећени информациони систем врати у што је могуће краћем року.

- **Корекције** – Стално унапређење уочених (интерно или екстерно) узрока који доводе или потенцијално могу довести до оштећења система

- **Опрезност и дисциплина** - Сви чланови организације морају да буду упознати са опасностима и морају да се придржавају сигурносних правила и регулатива – *ICT Security Policy*.

Успостављање функционалног надзора. Свака одбрамбена стратегија мора да има двостепени надзор над применом ИКТ стандарда и прописа. Ове послове треба да обављају најiskusнија и најстручнија лица. Контрола безбедности ИКТ мора бити постављена двостепено, и то:

- **Интерно** – спроводе лица задужена искључиво за безбедност у правосудним органима, и

- **Екстерно** - спроводе лица задужена за безбедност на нивоу Правосудног информаионог система.

Контроле безбедности ИКТ треба спроводити кроз:

- **Операционо функционалну контролу** – да ли систем ради коректно према пројектованом стању,

- **Контрола подобности** – да ли је пројектовани системи заштите адекватан, тј. да ли су испуњени неопходни предуслови за безбедан рад система.

- **Процена степена безбедности** – ову процену успоставити као периодичну са документованим начином спровођења процене.

Препорука је да се најмање квартално врши делимична процена операционе функционалности, а да се најмање годишње врши контрола подобности пројектованог решења. Обавезно је установити План опоравка од катастрофе (*Disaster Recovery Plan*). Циљ овог плана мора бити што мање време проведено у стању отказа појединих или свих функционалности система. Овај план је од непроцењиве важности за одржање континуитета пословања. План мора садржати опције за случајеве делимичног отказа система/функционалности и потпуног отказа/уништења капацитета. Плана изградити коришћењем “what-if” анализе. Потребно је дефинисати скуп критичних апликација, а све критичне апликације морају имати јасне процедуре за опоравак и враћање у потпуно функционално стање. План се пише једноставним експлицитним језиком, мора бити написан јасно и недвосмислено, да би био употребљив у тренутку незгоде када чиновници трпе велике психолошке притиске и нису потпуно концентрисани. План опоравка од катастрофе проверавати бар једном годишње симулирањем потпуног отказа система. Искуства са провере свакако ће послужити за реално сагледавање стања, свеобухватну анализу и унапређење свеукупне функционалности и безбедности система. Претње по безбедност Правосудног информационог система долазе и споља и изнутра. Заштита мора бити пројектована и изведена како ка споља тако и ка унутра. Потребно је успоставити систем потпуног праћења активности корисника. Неовлашћен приступ подацима и информацијама може се поделити у две групе:

Злонамерне

(осмишљене акције споља, изнутра или заједно)

Случајне

(непланирани неовлашћени упади у део система од стране запослених).

Злонамерне приступе потребно је тренутно и стриктно онемогућити. Систем пројектовати тако да појединачни неовлашћени упади могу да приступају само сепаратним подацима који не могу да чине информацију. Овакве упаде брзо онемогућити са тежњом да учинилац не схвати да је уочен. Потребно је информацију доставити врху система који се бави безбедношћу али и даље пратити и документовати све што се директно или индиректно тиче ове радње. Случајни упади у недозвољени део садржаја су можда још опаснији од злонамерних и потребно је обратити посебну пажњу на њих и то не због оних који су то учинили већ изстраха за цео информациони систем. Препорука је да се што је могуће више, документује уочено стање. Њихова појава може значити лоше пројектовање, увођење, администрирање. ... и овакве појаве се достављају управљачкој структури за безбедност Правосудног информационог система.

6.6 СТАНДАРД БЕЗБЕДНОСТИ ISO 27001

ИСО 27001 је настао као резултат потребе дефинисања међународно прихваћених норми, који ће својим захтевима дефинисати оквир формирања свеобухватног система заштите и циљеве његовог деловања како би се на ефективан и ефикасан начин управљало безбедношћу информација. Стандард ISO 27001 је конципиран у пет поглавља и то:

Систем за управљање безбедношћу

информација (ISMS),

Одговорност руководства,

Интерна провера ISMS,

Преиспитивање ISMS од стране руководства и Унапређење ISMS.

ISO 27001 је мултидисциплинаран, јер третира безбедности информација са три аспекта:

- **Информатиционог** – анализирајући и дефинишући

перформансе ИТ опреме, права приступа, криптовања,
лозинке, протоколе, политике са аспекта појаве ризика по
безбедност података и информација

- **Административног** – дефинишући јасна упутства, политике и
процедуре за генерисање информација, њихову
дистрибуцију, чување (складиштење)

- **Физичког** – физичка контрола приступа, евиденција запослених, видео надзор,
заштита радних просторија. Предности које имплементација и сертификација
ISO 27001 носи са собом, могу се сажети у два сегмента. Први сегмент је заштита и
безбедност информација кроз систематски и проактиван приступ за идентификовање и
деловање против читавог низа потенцијалних ризика којима су изложене информације
организације. Управљајући ризиком по безбедност информација, смањује се
вероватноћа појаве непредвиђених ситуација (претњи) на минимум.

Компоненте Безбедност информација:

Поверљивост (Конфиденцијалитет),
интегритета (Интегритет)
и доступности (Авајлабилитет) - PID (CIA).

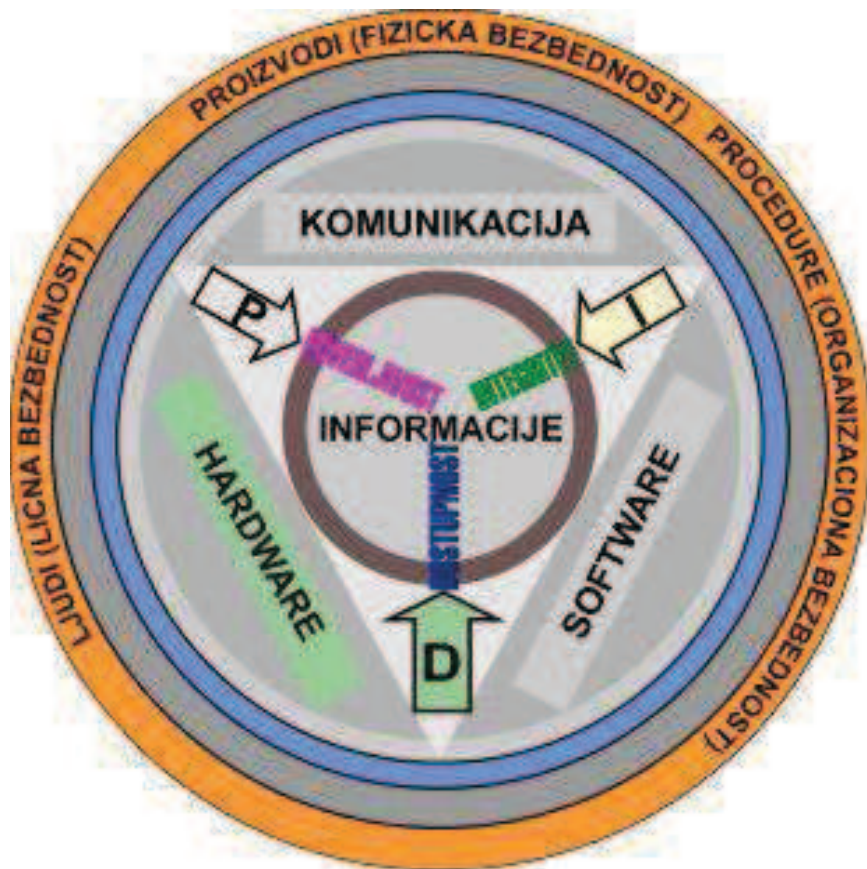
Информациони системи у том смислу групишу у три целине:

хардвер,
софтвер и

комуникације са циљем да се идентификују и примене стандарди безбедности
информација, као и механизми заштите и превенције, на три нивоа, или слојева:

физички,
лични и

организациони (Слика 27.). У суштини, процедуре или правила се спроводе да кажу
службеницима (администратору, кориснику и оператеру) како да користе ИКТ како би
се осигурала безбедност информација у оквиру Правосудног информационог система.



Слика 27. Компоненте безбедности информација

Добити које имплементација Система менаџмента безбедности информација (ISMS), сагласно захтевима ISO 27001:2005, у Правосудни информациони систем могу бити следеће:

- **Јуст-ин-тима ефекат** – Права информација - на право место - у право време
- **Заштита и очување know-how**
- **Повећање ефективности и ефикасности система**

- Повећање пословног кредибилитета и поверења од стране клијената и партнера
- Уштеда времена рационализацијом количине и садржине информација
- Оптимизација ресурса потребних за дистрибуцију и чување података
- Рана идентификација рањивости, претњи и потенцијалних негативних утицаја на пословање
- Смањење ризика од запошљавања људи који би могли нашкодити систему
- Постизање синергетског ефекта тимског рада
- Промптна усклађеност са законском регулативом
- Бржи проток информација између запослених
- Стварање предуслова за одређивање одговорности
- Смањење неспоразума код запослених услед "укрштања информација"

Значајне су користи које модел за уређење система за безбедност информација ISO 27001 остварује организацијама које се одлуче да га имплементирају, пре свега у смислу побољшавања својих организационих перформанси. Извесно је да овај модел представља најбољу праксу у области заштите и безбедности информација која је преточена у захтеве стандарда.

6.7 ПОЛИТИКА ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ У ПРАВОСУЂУ

Политика информационе безбедности су посебна врста документованих пословних правила за заштиту података и система који складиште и обрађују информације. У одељку 5 ISO/IEC 27002:2005 **Information technology -Security techniques - Code of Practice for Information Security Management** дефинисана је Политика информационе безбедности (*ICT Security Policy*). Менаџмент треба да дефинише свеобухватан пакет детаљније корпоративне политике безбедности информација, у виду информација за кориснике безбедносне политике. Политика информационе безбедности је описана кроз 39 контрола циљева стандарда ISO/IEC 27002 који су направили одличан свеобухватан али и сажет скуп аксиома политике. Садржај је прилагођен да одражава оно што руководство заправо жели да постигне у односу на пословне организације циљева безбедности. Два су приступа дефинисању Политике информационе безбедности:

1. Појединачне политике покривају специфична питања безбедности као што су "политика Емаил сигурности" и "политика лозинки". Оне дефинишу одговорност и сигурност кључних група, функција и тимови људи. Требало би да те политике буду референтне на вишим и нижим нивоим хијерархије политике.

2. Свеобухватна политика за кориснике који садржи језгровите политике изјава за одражавање целе ISO/IEC 27002, са бројним уграђеним унакрсним референцама између повезаних политика изјава и позивање на везе аксиома, стандарда, процедура и смерница. За потребе Правосудног информационог система важно је изградити и појединачне и свеобухватне политике, због сложености организације и лакшег управљања информационом безбедношћу. Политике информационе безбедности, принципи и детаљне политике, треба да буде формално прегледане и усвојене од стране вишег руководства које треба да прихвати читав програм ИКТ безбедности јер ће довести до промене дотадашње праксе у целој организацији. Највише руководство мора бити свесно општих циљева и подржати промене. Политика безбедности података, стандарда, процедура и смерница никада се неће заиста "завршити" већ је потребно да се ажурирају с времена на време и да прате промене унутар и изван организације (нпр. појава нових претњи безбедности информација може бити повод за измену постојећих политика и сл. или бар генерацију додатних материјала безбедносне свести о промени претњи). Међусобни однос процедура, стандарда, полиса, аксиома и

принципа безбедности ISO/IEC 27002 као и садржаја Упутства о информационој безбедносној политици и корпоративне информационе безбедносне политике дат је на Пирамиди безбедности, слика 28. Потпун приступ безбедности мора садржати принципе, аксиоме, полисе, стандарде и процедуре и упутства којима се потпуно дефинише безбедност.



Слика 28. Пирамида безбедности

Standardom je trenutno definisano 39 kontrolnih ciljeva

standarda ISO/IEC 27002 – aksioma koji opisuju

Politiku informacione bezbednosti kao što sledi:

- *Information Security Overview*
- *Acceptable Use Policy*
- *Analog Line Policy*
- *Backup Procedures Policy*

- *Business Continuity Plan (BCP) Policy*
- *Computer Lifecycle Program (CLP) Policy*
- *Data Breach Policy*
- *Data Classification Policy*
- *Data Collection Policy*
- *Data Lifecycle Policy*
- *Data Storage Policy*
- *Database Credentials Policy*
- *Digital Signature Policy*
- *Disaster Recovery Plan (DRP) Policy*
- *Electronic Mail (e-mail) Retention Policy*
- *Encryption Policy*
- *Firewall Security Policy*
- *Identity Theft Prevention Policy*
- *Incident Response Policy*
- *Information Asset Issue Policy*
- *Information Assurance (IA) Policy*
- *Information Security Management System (ISMS) Policy*
- *Intranet Policy*
- *Malicious Software (Malware) Policy*
- *Non-Regulatory Compliance Policy*
- *Operating System Policy*
- *Operational/Technical/Management Security Policy*
- *Password Policy*
- *Personal Communication Device (PCD) Policy*
- *Personal Use Policy*
- *Privacy & Monitoring Policy*
- *Regulatory Compliance Policy*
- *Remote Access Policy*
- *Risk Assessment Policy*
- *Router Security Policy*
- *Service Provider Policy*

- *User Security Training Policy*
- *Vulnerability Assessment Policy*
- *Wireless Communications Policy*

Наведене политике су свакако смернице за дефинисање свих питања везаних за безбедност Правосудног информационог система. Уколико постоје још неке специфичности које не спадају у наведених 39 аксиома безбедности препоручује се да се додају као посебне политике безбедности у додатку. Поред аксиома безбедности, Политика информационе безбедности мора садржати и следеће прилоге:

- **Термини и дефиниције**
- **Обрасци и упутства о признању политике сигурности**
- **Попис корисничке опреме – пријем, издавање**
- **Формулари споразума о чувању поверљивих информација за оутсорсинг послове**
- **Формулари за реаговање у инцидентним ситуацијама**
- **Налози за именовање главних/ог службеника за безбедност информација**
- **Усклађеност са законима**
- **Упутства међународне организације за стандарде**
- **Политика сигурности информација, приручник, документација**

Наведени прилози представљају онај део који је намењен корисницима у систему и треба својим садржајем да отклони све недоумице у раду корисника. Ови документи тако и требају да буду конципирани, како би корисник у некој од кризних ситуација по

ИКТ систем, могао да реагује на најбољи начин. Кориснику треба објаснити да иза његове улоге у проесу стоји цео ИКТ систем који захтева реаговање по одређеним процедурама и правилима. Након упознавања са свим садржајима који су од интереса за одређеног корисника, у прилозима се налазе и обрасци о одговорности корисника, које сваки корисник у оквиру организације мора да потпише.

6.8 ПРЕПОРУКЕ ЗА МОНИТОРИНГ БАЗА ПОДАТАКА

Да би се сагледала целину информационог система и апликативних система у њима путем којих се смештају подаци у базу података, треба поћи од безбедносних решења, која се у најопштијем смислу могу посматрати са три аспекта :

A1) Провера приступа апликативном систему (аутентификација корисника),

A2) Обезбеђење потпуне функционалности апликативног система кроз проверу акција и привилегија извршавања од стране корисника у раду са изабраном функционалношћу (ауторизација корисника),

A3) Обезбеђење интегритета података кроз проверу привилегија над подацима.

У том смислу потребно је да се, при пројектовању апликативног система, посебно разматра и пројектује функција сигурности узимајући у обзир горе наведене аспекте. Када се каже пројектовање функције сигурности мисли се на класичну функционалну анализу као и дефинисање модела података сигурносног модула у односу на све наведене аспекте са почетка текста. Провера уласка у апликативни систем подразумева функцију контроле уласка корисника у апликацију (аутентификација корисника). Јасно је да је у моделу података за овај аспект потребно прво дефинисати све кориснике (у табелама за УСЕР-е) којима ће се доделити право уласка у апликативни систем. Провера акција и привилегија извршавања, као део сигурносног модула, омогућава да се на основу пројектованих улога у апликативном решењу (датих у табелама које описују улоге) и везама са конкретним апликативним модулима верификују привилегије корисника над одређеном функционалношћу. Из овога следи да се улоге

могу доделити само већ дефинисаним корисницима, односно усерима који имају право уласка у апликацију. Ради лакшег рада са улогама потребно је водити рачуна о механизмима наслеђивања улога. Обезбеђење интегритета података кроз проверу привилегија

над подацима је део сигурносног модула који омогућава контролу рада над већ унетим подацима. Његов модел података се такође ослања на већ дефинисане кориснике. Одређеним корисницима се додељују привилегије и улоге и уз помоћ тих механизма имају право рада над већ унетим подацима. Посебан сегмент у оквиру овог дела сигурносног модула је контрола приказивања података који у моделу података такође има своје улоге и привилегије. За сва три горе описана аспекта потребно је дефинисати функцију непорецивост активности којом се кроз табеле архива активности (у моделу података сигурносног модула) хронолошки прати рад корисника у систему. Описани аспекти безбедности покривају примарне безбедоносне циљеве (расположивост, интегритет и поверљивост) дате у скупу циљева заштите у релевантним стандардима заштите

(SRPS ISO/IEC 27001, BS 25999, NIST,...). У домену система управљања квалитета пословања потребно је утврдити ледеће категорије мера:

- **Потврда природе и степена инцидента,**
- **Преузимање контроле и координација реакције на инцидент**
- **Комуникација са интересним странама, и**
- **Обнављање активности организације.**

Ово је најопштије сагледавање безбедности у апликативном слоју. Међутим, како апликативни слој директно зависи од базе података, односно оперативног система као носиоца базе и средњег слоја, то је и безбедност апликативног решења директно зависна од сигурносних пропуста у слоју оперативног система. Наиме, како је основни концепт у раду информационих система да виши слој програма прихвата сервисе из нижег слоја (оперативни систем, базе података, средњи слој, апликација) то је и

заштита виших слојева директно зависна од заштите на нижим слојевима. Другачије речено, онај ко контролише оперативни систем практично контролише и све слојеве изнад њега. Начин понашања правосудних органа и појединаца који имају приступ базама података правосуђа могу да укажу на озбиљне проблеме који могу утицати на безбедност, приватност, поверљивост и доступност

података. Потребно је да се развије систематски процес за мониторинг ових понашања, као и да се спроводе контроле како би се ублажили ризици у вези са базама података. У наставку је дат преглед потенцијалних корисника у једном систему са њиховим могућим начинима приступа подацима похрањеним у базама података. Уз сваки од ових начина дате су и препоруке за неутралисање ризика:

а) ПРИВИЛЕГОВАНИ КОРИСНИЦИ

Корисници са посебним овлашћењима, на високом нивоу привилегије - администратори база података и систем администратори - треба увек да буду предмет интензивног испитивања у организацији са аспекта безбедности и то од посебног лица задуженог за безбедност. Разлог за наведене радње је очигледан јер ови корисници имају увид и приступ свим подацима и основама система, тако да потенцијално могу да причине огромну штету. Они треба да буду предмет ригорозних рутинских провера, и треба да се прате и ревидирају за следеће потенцијалне проблеме/активности:

- Приступ, брисање или промена података,
- Приступ преко неодговарајућих или неодобрених канала,
- Шема модификације,
- Неовлашћено додавање корисничких налога или модификација постојећих налога.

б) КРАЈЊИ КОРИСНИЦИ

Крајњи корисници - физичка лица који имају легитиман приступ подацима кроз неку

врсту примене пословне апликације нпр. суда представљају озбиљан ризик за намерне и несвесне злоупотребе тих података у судском, односно шире посматрано правосудном систему. Безбедносни стручњаци би требало да уложе посебну пажњу на три потенцијална проблема понашања:

- **Пристап прекомерној количини података или подацима који нису потребни за свакодневни додељени рад,**
- **Пристап подацима ван стандардног радног времена,**
- **Пристап преко неодговарајућег или неодобреног канала.**

ц) ПРОГРАМЕРИ, СИСТЕМ АНАЛИТИЧАРИ, АДМИНИСТРАТОРИ

Ови корисници представљају две посебне врсте ИКТ ризика. Први ризик је потенцијал за повреде података као и компромитовање интелектуалне својине или личних приватности. Ови корисници због природе свог посла морају да имају изузетно висок ниво привилегија за пристап. Много озбиљнији проблем је што ови технички највештији запослени у суду имају могућност приступа или промена делова система који су у живој продукцији, што може довести до лошег рада, падова система и, у неким случајевима, диригованим безбедносним пропустима. Примарно понашање ИКТ кадра у судовима на које би требало обратити пажњу је:

- Пристап живим подацима у пословним системима.

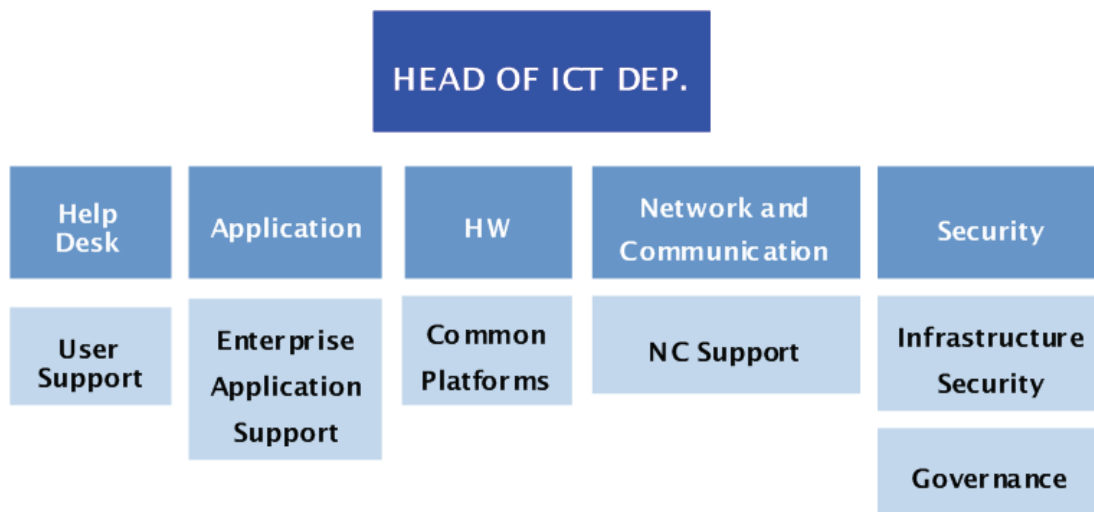
д) ИКТ ОПЕРАЦИЈЕ -ИКТ пословање судова, не само појединачних запослених, али и процеси за које је одговоран суд имају значајан утицај на правилно функционисање и управљање базама података хијерархијски нижих судова. Њихове базе података везане су за активности које треба да буду ревидиране у две кључне области:

- **Неодобрене промене на базама података или апликацијама,**
- **Ванциклусне закрпе пословног систем**

6.9 ПРЕДЛОГ ЗА ПОБОЉШАЊЕ ЗАШТИТЕ ИНФОРМАЦИОНОГ СИСТЕМА

Политика безбедности података, стандарда, процедура и смерница никада се неће заиста "завршити" већ је потребно да се ажурирају с времена на време и да прате промене унутар и изван организације (нпр. појава нових претњи безбедности информација може бити повод за измену постојећих политика и сл. или бар генерацију додатних материјала безбедносне свести о промени претњи) [20]. Информациона безбедност у савременом свету постала је један од основних проблема цивилизације, а њено угрожавање потиче од злоупотреба информационо комуникационих технологија, малициозних кодова, уништавања и губљења података, *cyber* криминала, злоупотребе личних података, и других илегалних радњи. Организација дирекције за ИКТ која се стара о правосудном информационом систему требала би да има следеће организационо-функционалне целине:

- подсистем подршке,
- апликативни подсистем,
- ХВ подсистем,
- подсистем мреже,
- подсистем безбедности.



Слика 29. Организација ИКТ сектора за подршку безбедности.

Успостављање подсистема безбедности неизоставни је део тежње ка успостављању

потребног нивоа безбедности у правосудном информационом систему. Свест о информационој безбедности у Правосудном информационом систему је недовољно развијена јер су доносиоци одлука лица са основним знањем из области

ИКТ, са непознавањем и потцењивањем потенцијалних опасности. Постоји одсуство шире стручне анализе и критике стања безбедности, мало јавних е-сервиса. Приметна је пасивност државе у развоју и увођењу нормативног оквира за информациону безбедност и примену постојеће позитивне правне регулативе. Безбедност није само технолошка функција већ је и правно процедурални оквир базиран на организационим променама.

ЗАКЉУЧАК

Савремено правосуђе уводи електронске сервисе како би повећале ефикасност функционисања правосудних органа али и како би пружио лакши начин размене и прибављања информација или остваривања одређених функционалности у интерним процедурама или у остваривању права грађана. Успостављени системи и сервиси електронског правосуђа морају бити на највишем нивоу безбедности. Информациони систем представља начин обраде информација а са циљем правовременог добијања сазнања неопходних за даље деловање. Под Информационим системом подразумевају се међусобно и функционало повезани процеси прикупљања, преношења, обраде, коришћења и чувања података. Потреба за увођењем информационог система се огледа у могућности покривања свих информационих токова у управљању одређеним Пословним системом, у складу са природом и задацима који се обављају у систему. Од Информационог система се очекује да обезбеди основу за извршавање различитих задатака и захтева које учесници постављају систему. Тиме се исказује потреба за комплексним и ефикасним информационим технологијама неопходним за изградњу и функционисање Информационог система. Повезивање под система Информационог система у јединствену, функционалну и економичну целину, постиже се помоћу база или банке података, у оквиру којих се меморишу сви релевантни подаци неопходни за функционисање Пословног система. Наш информациони систем је објединио велики део потребних пословних процеса који су неопходни за функционисање овог државног органа. [21]

ЛИТЕРАТУРА

- [1] Проф.др Ангелина Његуш, Пословни информациони системи треће издање Београд 2009
- [2] http://shomi91.blogspot.com/2012/11/hardver-softver_16.html
- [3] <http://sveoracunarima.wordpress.com/category/hardver/>
- [4] Breza Software Engineering, Документ Администрација система Београд 2009
- [4] Драган Товаришић дипл.инж.ел Информациони систем Железнице Суботица , 2012
- [5] http://www.znanje.org/knjige/computer/access/access_01/FUNKCIJE%20INFORMACIONOG%20SISTEMA.htm
- [6] Драган Товаришић дипл.инж.ел Информациони систем Железнице Суботица , 2012
- [7] Доц. др Саша Иванов, Информациони ресурси и информациони системи
- [8] <http://www.propisi.com/zakon-o-oduzimanju-imovine-proistekle-iz-krivnog-dela.html>
- [9] http://paragraf.rs/propisi/zakon_o_oduzimanju_imovine_proistekle_iz_krivnog_dela.html
- [10] Breza Software Engineering, Solution documentation for runtime software version Београд 2012
- [11] Документ представља корисничку спецификацију подсистема Управљање одузетом имовином verzija 1.0 author Breza Software Engineering
- [12] Проф.др Ангелина Његуш, Развој апликације са сервисно оријентисаном архитектуром (SOA), Београд 2010
- [13] <http://www.zimbio.com/Computer+programming/articles/FQuGk0cQ3rb/ADF+Framework+JDeveloper+Driving+Force+Behind>
- [14] <http://msforge.net/blogs/blackdwarf/archive/2008/02/24/mvc-framework-i-sva-njegova-lica.aspx>
- [15] [http://onlineappsdba.com/index.php/2010/04/06/upgrademigrate-oracle -](http://onlineappsdba.com/index.php/2010/04/06/upgrademigrate-oracle-)

internet-application-server-ias-9i10g-to-oracle-weblogic-serverfmw-11g /

- [16] Breza Software Engineering Опште упутство за рад са апликацијом 2012
верзија 1.5
- [17] Funkcionalne preporuke za uspostavljanje pravosudnog informacionog
sistema Mr. Rade Dragović 2010
- [18] Politika bezbednosti i preporuke za povećanje bezbednosti baza podataka
u pravosudnom informacionom sistemu mr. RadeDragović 2012
- [19] Politika bezbednosti pravosudnog informacionog sistema
mr.Rade Dragović 2011
- [20] Preporuke za unapređenje bezbednosti baza podataka u
pravosudnom informacionom sistemu mr. Rade Dragović 2012
- [21] http://www.znanje.org/knjige/computer/access/access_01/POJAM%20INFORMACIONOG%20SISTEMA.htm