KRIPTOGRAFSKA REŠENJA ZAŠTITE MEMORIJE ORGANIZACIJE SA STANOVIŠTA MENADŽMENTA ZNANJA

By Dragan Savić

WORD COUNT 104836 TIME SUBMITTED 15-MAR-2021 10:21AM
PAPER ID 69965566

UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

DOKTORSKE STUDIJE
STUDIJSKI PROGRAM: NAPREDNI SISTEMI ZAŠTITE

KRIPTOGRAFSKA REŠENJA ZAŠTITE MEMORIJE ORGANIZACIJE SA STANOVIŠTA MENADŽMENTA ZNANJA

- doktorska disertacija -

Mentor:
prof. dr Mladen Veinović

Kandidat:
ms Dragan Savić

Beograd, 2021.

Univerzitet Singidunum

UNIVERSITY OF SINGIDUNUM
DEPARTMANT OF POSTGRADUATE STUDIES

DOCTORAL STUDY
PROGRAM: ADVANCED PROTECTION SYSTEMS

CRYPTOGRAPHIC SOLUTIONS OF ORGANIZATION'S MEMORY PROTECTION FROM THE POINT OF MANAGEMENT'S KNOWLEDGE

- doctoral dissertation -

Mentor:
Mladen Veinović, PhD

Candidate:
Dragan Savić, ms

Belgrade, 2021

Univerzitet Singidunum

4

Podaci o mentoru i članovima komisije

Mentor:

Prof. dr Mladen Veinović, redovni profesor
Univerzitet Singidunum

Članovi komisije:

Prof. dr Mladen Veinović, redovni profesor, mentor
Univerzitet Singidunum

Prof. dr Milan Milosavljević, redovni profesor
Univerzitet Singidunum

Prof. dr Petar Spalvic, redovni profesor
Univerzitet u Prištini sa privremenim sedištem u K. Mitrovici

Datum odbrane:

Univerzitet Singidunum

Podaci o doktorskoj disertaciji

Naziv disertacije: **Kriptografska rešenja zaštite memorije organizacije sa stanovišta menadžmenta znanja**

Rezime

Moderne kompanije se svakim danom suočavaju sa problemom opterećenosti velikom količinom informacija i podataka, a što otežava njihovo poslovanje i donošenje efikasnih poslovnih odluka. Pronalaženje nove suštine primene načina menadžmenta znanja u smislu efikasnog korišćenja memorije organizacije (znanja), predstavlja sve veću potrebu kompanija da unaprede svoje poslovanje. Isto tako, zaštita načina pristupanja memoriji organizacije (znanju kompanije), njegovoj razmeni i upravljanju njime, kompanije sve više posvećuju pažnju i stavljaju akcenat u svom poslovanju. Primena koncepta poslovne inteligencije u upravljanju memorije organizacije postaje neizostavan element strategije uspešnih kompanija. Integrisano automatizovano upravljanje memorijom organizacije (znanjem jedne kompanije), iako veoma složeno, predstavlja rešenje za interakciju menadžmenta znanja i informacione tehnologije. Time se stvara mogućnost potpunog objašnjavanja procesa donošenja odluka u jednoj kompaniji, ali i procesa toka dokumenata, informacija i podataka. Integrisanim automatizovanim upravljanjem memorijom organizacije, kompanija ostvaruje mogućnost dobijanja detaljnih podataka na osnovu kojih je olakšano konkretno poslovno odlučivanje. Takođe, ovde se javlja i zahtev za zaštitu jednog takvog integrisanog automatizo vanog procesa. U skladu sa određenim i usvojenim međunarodnim standardima (ISO 27001), menadžment u ovakvom sistemu kakav je memorija organizacije treba da osigura efikasnu implementaciju, praćenje i unapređenje sistema za rukovanje bezbednošću memorije organizacije.

Zaštita i bezbednost memorije organizacije kroz kriptografska rešenje treba da zadovolji balans između zahteva korisnika, funkcionalnosti unutar memorije organizacije i potrebe zaštite osetljivih podataka i čuvanje njihovog integriteta. Ovakav integrisani automatizovani proces upravljanja memorijom organizacije predstavlja jedno rešenje koje bi svoju upotrebu moglo da nađe kako u oblasti učenja inteligentnih sistema, tako i u postojećim sistemima savremenog poslovnog odlučivanja. Jedan od predloženog načina rešenja zaštite integrisanog sistema za proces upravljanja memorijom organizacije u ovom radu biće i mogućnost snimanja u šifrovanom obliku, čime podaci postaju dostupni samo kroz informacioni sistem kompanije. U ovom radu biće predstavljeno sopstveno kriptografsko rešenje zaštite memorije organizacije sa stanovišta menadžmenta znanja. Pristup dokumentima i podacima će imati samo ovlašćeni korisnici sistema na osnovu definisanih dozvola pristupa. Autentičnost dokumenata i njihova nepromenljivost bi se obezbedila pomoću digitalnih potpisa, što predložena kriptografska rešenja obezbeđuju u skladu sa aktuelnim zakonskim propisima za elektronski dokument. Isto tako, biće razmotreni principi i modeli koji obezbeđuju i zaštitu podataka i privilegovan pristup podacima, a sve u cilju donošenja odluka zasnovanih na memoriji organizacije. Najbolji primer za ovakvu analizu su bezbednosno-informativne agencije, a brojni su primeri, kako dobrih organizacija, tako i propusta u njihovom radu.

Univerzitet Singidunum

Ključne reči: kriptografija, zaštita podataka, memorija organizacije, menadžment znanja, algoritam, napad, simetrično i asimetrišno šifrovanje, digitalni potpis.

Naučna oblast: Računarske nauke

Uža naučna oblast: Računarstvo i informatika

UDK broj:

Univerzitet Singidunum

Information about the thesis

Title of thesis: **Cryptographic solutions of organization's memory protection from the point of management's knowledge**

Summary

Every day modern companies are facing the problems of overload of information and data and that makes hard for them to run a business and to make effective business decisions. It is necessary for companies to find a good way of implementing the management knowledge in order to improve the business activity. Moreover, the protection of the way of accessing organizational memory (the knowledge of the company), his trade and management of it is the new approach on which companies pay more attention to. The implementation of the concept of management intelligence, in order for companies to manage the organizational memory, becomes indispensable element of the successful companies' strategies. Integrated automated organizational memory management (knowledge of one company), although very complex, is a solution for the interaction of knowledge management and information technology. In that way, it is easier for a company to explain the process of making decision in one company, but also for the flow of documentation, information and data. With the integrated automated memory management of the organization, the company sees the possibility of obtaining detailed data based on which concrete business decision-making is facilitated. Moreover, here comes the request for the protection of one such integrated automated process. In accordance with certain adopted international standards (ISO 27001), management in such systems as the organization's memory ,should provide a model for establishing the implementation, handling, monitoring, review, maintenance and improvement of the organization's memory security management system.

Protection and security of the organization's memory through a cryptographic solution should satisfy the balance between user requirements, functionality within the organization's memory and the need to protect sensitive data and preserve their integrity. This integrated automated process of memory management of the organization is a solution that could find its use both in the field of learning intelligent systems and in existing systems of modern business decision making. Digital signing would ensure the indisputability of documents and their immutability, which the proposed cryptographic solutions provide in accordance with the current legal regulations for electronic documents. In this paper, one of the proposed ways to protect the integrated system for the process of memory management of the organization will be the possibility of recording them in encrypted form. This will make the data available only through the company's information system. This paper will present the organization's own cryptographic solution for memory protection from the point of view of knowledge management. Access to documents and data would be available only to system users who are explicitly authorized to do so through the access to permission management system. Digital signing would ensure the indisputability of documents and their immutability, which the proposed cryptographic solutions provide in accordance with the current legal regulations for electronic documents. Principles and models that provide both data protection and privileged access to data will be discussed, all with the goal of making decisions based on the organization's memory. The best example for such an analysis are security information agencies, and there are numerous examples of both good organizations and omissions in their work.

Ključne reči: cryptography, data protection, organization memory, knowledge management, algorithm, attack, symmetric and asymmetric encryption, digital signature.

Scientific field: Computer Science

Scientific Area: Computers and IT

UDK Number:

SADRŽAJ

1. Uvod ____ *6*

1.1 Metodološke osnove istraživanja ____ **7**
1.1.1 Predmet i cilj istraživanja ____ 7
1.1.2 Istraživačke hipoteze ____ 10
1.1.3 Metode istraživanja i tok istraživačkog postupka ____ 10

1.2 Očekivani rezultati istraživanja i naučni doprinos ____ **11**

1.3 Pregled sadržaja po poglavljima ____ **12**

2. Teorija znanja ____ *15*

2.1 Podatak, informacija, znanje ____ **15**
2.1.1 Pojmovno određivanje znanja ____ 17
2.1.2 Kategorizacija znanja ____ 18
2.1.2.1 Eksplicitno i prećutno znanje ____ 18
2.1.2.2 Individualno i organizaciono (kolektivno) znanje ____ 20

2.2 Niz međusobnih interakcija u kreiranju inovacije znanja ____ **23**

2.3 Strategije menadžmenta znanja ____ **25**
2.3.1 Generičke strategije menadžmenta znanja ____ 25
2.3.2 Opšte strategije menadžmenta znanja ____ 26
2.3.3 Elementi strategije menadžmenta znanja ____ 26
2.3.4 Izrada strategije menadžmenta znanja ____ 28

2.4 Ekonomija znanja ____ **30**
2.4.1 Prednosti primene menadžmenta znanja ____ 31
2.4.2 Prepreke i poteškoće u menadžmentu znanja ____ 32

3. Menadžment znanja ____ *34*

3.1 Definicija menadžmenta znanja ____ **34**

3.2 Koncepti menadžmenta znanja ____ **35**
3.2.1 Intelektualni kapital ____ 36
3.2.2 Menadžment znanja i intelektualni kapital ____ 38
3.2.3 Znanje kao nevidljiva imovina kompanije ____ 39

3.3 Elementi menadžmenta znanja ____ **40**

3.4 Modeli menadžmenta znanja ____ **41**

3.5 Implementacija menadžmenta znanja u praksi - Metode menadžmenta znanja ____ **43**
3.5.1 Brainstorming ____ 43
3.5.2 Učenje i prikupljanje ideja *(Learning and Idea Capture)* ____ 44
3.5.3 Uključivanje znanja u projekat *(Peer Assists)* ____ 44
3.5.4 Pregled naučenog *(Learning Reviews)* ____ 44
3.5.5 Naknadna ocena aktivnosti *(After Action Review)* ____ 45
3.5.6 Međusobno podučavanj *(Collegial Coashing)* ____ 46
3.5.7 Mentorstvo *(Mentoring)* ____ 46
3.5.8 Sistem najbolje prakse *(Good practice)* ____ 46
3.5.9 Izlazni intervju *(Exit Interview)* ____ 47
3.5.10 Pričanje priča *(Storytelling)* ____ 47
3.5.11 Kafe znanja *(Knowledge Cafe)* ____ 48
3.5.12 Zajednica prakse *(Community of Practice)* ____ 49
3.5.13 Sajam znanja (Knowledge Fair) ____ 50
3.5.14 Žute strane *(Yellow Pages)* ____ 50

3.5.15 Posebne vrste baze znanja *(Wikis)* 51
3.5.16 Blog 51

3.6 Tehnologije i alati za menadžment znanja 52

3.7 Perspektive koncepta menadžmenta znanja 54

4. Konceptualna tehnološka infrastruktura 56

4.1 Reinženjering 56

4.2 Uvođenje savremene organizacione strukture u kompaniji 57
4.2.1 Funkcionalna organizaciona struktura 58
4.2.2 Procesna organizaciona struktura 58
4.2.3 Projektno organizaciona struktura 58

4.3 Procesni pristup 59

4.4 Razvijen informcioni sistem kompanije 60
4.4.1 Razvoj informacionih sistema 60
4.4.2 Transakcioni informacioni sistem 60
4.4.3 Sistemi za podršku odlučivanju 61
4.4.4 Izvršni informacioni sistemi i izvršni sistemi podrške 64
4.4.5 Ekspertni sistemi 66
4.4.6 Sistemi za upravljanje (menadžment) dokumentima 68

4.5 Informacioni sistemi za kreiranje znanja u kompanijama 70

4.6 Struktura Interneta i e-dimenzija menadžmenta znanja 73

4.7 Organizacija koja uči 74

4.8 Sistem poslovne inteligencije 76

5. Rudarenje podataka / Data Mining 79

5.1 Pojam rudarenja podataka 79
5.1.1 Zadaci (problemi) rudarenja podataka 81
5.1.2 Rudarenje podataka i otkrivanje znanja 81
5.1.3 Koraci u procesu rudarenja podataka – otkrivanje znanja 82

5.2 Priprema podataka za rudarenje 84
5.2.1 Pretprocesuiranje podataka 84
5.2.2 Analiza relevantnosti atributa 84
5.2.3 Završni postupci 85

5.3 Tehnike rudarenja podataka 86
5.3.1 Metoda regresije 86
5.3.2 Klasifikacione metode 86
5.3.3 Metode klasterovanja 87
5.3.4 Neuronske mreže 88
5.3.5 Stablo odlučivanja 90
5.3.6 Metode za analizu veza (asocijativna pravila) 91
5.3.7 Genetski algoritmi 91

5.4 Korišćenje znanja otkrivenog u procesu rudarenja podataka 92

5.5 Područja za primenu alata za rudarenje podataka 93

6. Memorija organizacije 95

6.1 Definicija memorije organizacije 95

6.2 Upravljanje memorijom organizacije 97

6.3 Tipologija memorije organizacije 99

6.4 Informatičke pretpostavke za formiranje memorije organizacije 99

6.5 Stvaranje memorije organizacije 103
6.5.1 Nekompjuterizovana memorija organizacije 104
6.5.2 Memorija organizacije bazirana na dokumentima 104
6.5.3 Memorija organizacije bazirana na menadžmentu znanja 105
6.5.4 Memorija organizacije zasnovana na slučajevima 106
6.5.5 Izgradnja distribuirane memorije organizacije 107
6.5.6 Kombinacija tehnika u izgradnji memorije organizacije 108

6.6 Korišćenje memorije organizacije 108

6.7 Ocenjivanje memorije organizacije 109

6.8 Održavanje i razvoj memorije organizacije 110

6.9 Problemi upravljanja sa velikom količinom podataka 111
6.9.1 Big Data sistemi 111
6.9.1.1 Pojava, definicija i karakteristike „Big Data" sistema 111
6.9.1.2 „Big Data" tehnike za rad 114
6.9.1.3 „Big Data" tehnologije za rad u praksi 114
6.9.1.4 Faktori koji utiču na primenu „Big Data" tehnologija 116
6.9.1.5 Negativne implikacije upotrebe „Big Data" tehnologija 117
6.9.1.6 Značaj „Big Data" tehnologija 118
6.9.2 Sistemi za planiranje poslovnih resusrsa – ERP sistemi 119
6.9.2.1 Definicije ERP sistema 119
6.9.2.2 Evolucija ERP sistema 121
6.9.2.3 Arhitektura ERP sistema 121
6.9.2.4 Karakteristike ERP sistema 123
6.9.2.5 Implementacije ERP sistema 123
6.9.2.6 Standardi tehnologije realizacije ERP sistema 125
6.9.2.7 Rešenja ERP sistema 125
6.9.2.8 Prednosti i nedostaci ERP sistema 126
6.9.3 Data Warehouse sistemi 127
6.9.3.1 Osnovni okviri skladišta podataka 127
6.9.3.2 Cilj realizacije skladišta podataka 127
6.9.3.3 Osnovne funkcije skladišta podataka 128
6.9.3.4 ETL procesi 128
6.9.3.5 Ekstrakcija podataka 130
6.9.3.6 Proces transformacije podataka 130
6.9.3.7 Proces punjenja skladišta podataka 132
6.9.3.8 Izbor arhitekture ETL sistema 132
6.9.3.9 Osnovni modeli skladišta podataka 133
6.9.3.10 Dvoslojna arhitektura sa zajedničkim skladištem podataka 134
6.9.3.11 Dvoslojna arhitektura sa više nezavisnih lokalnih skladišta podataka 134
6.9.3.12 Troslojna arhitektura skladišta podataka 134
6.9.3.13 Implementacija skladišta podataka u poslovne subjekte 135
6.9.3.14 Višedimenzionalni prikaz podataka 136
6.9.4 Računarstvo u oblaku – *Cloud Computing* sistemi 138
6.9.4.1 Definisanje računarstva u oblaku 138
6.9.4.2 Koncepti karakteristike računarstva u oblaku 139
6.9.4.3 Arhitektura računarstva u oblaku 140
6.9.4.4 Modeli usluga računarstva u oblaku 140
6.9.4.5 Modeli implementacije računarstva u oblaku 142
6.9.4.6 Problemi i rizici bezbednosti računarstva u oblaku 143
6.9.4.7 Prednosti i nedostaci računarstva u oblaku 144
6.9.5 Hadoop sistemi 145
6.9.5.1 Bazne komponente Hadoop platforme 145
6.9.5.2 Eko-sistem Hadoop 148
6.9.5.3 Prednosti korišćenja Hadoop 148

7. Optimizacija zaštite memorije organizacije *149*

7.1 Pretnje i ranjivosti memorije organizacije 149

7.1.1 Bezbednosne pretnje 149
7.1.2 Procena ranjivosti 151
7.1.3 Procena rizika 152
7.1.4 Ograničenja pri izboru mera zaštite 153

7.2 Sofistikacija malvera 154
7.2.1 Trojanski konji 155
7.2.2 Virusi 155
7.2.3 Kompjuterski crvi 157
7.2.4 Adware 158
7.2.5 Spyware 158
7.2.6 Bot 158
7.2.7 Bug 159
7.2.8 Ransomware 159
7.2.9 Rootkit 161

7.3 Napadi 161
7.3.1 Napadi nultog dana 161
7.3.2 Ciljani napadi 163
7.3.3 Interni napadi 167

7.4 Zaštita kontejner tipa 169
7.4.1 Antivirusna zaštita 169
7.4.1.1 Metode antivirusnih softvera 169
7.4.1.2 Organizacione mere antivirusne zaštite 170
7.4.1.3 Antivirusni programi 171
7.4.2 Firewalls zaštita 172
7.4.3 IDS/IPS zaštita 174
7.4.3.1 IDS zaštita – Sistem za detekciju upada 174
7.4.3.1 IPS zaštita – Sistem za prevenciju upada 176
7.4.3.1.1 HIPS – IPS za zaštitu pojedinih računara 177
7.4.3.1.2 NIPS – IPS za zaštitu mreže 178
7.4.3.1.3 Metode detekcije napada 179
7.4.3.1.4 Karakteristike IPS nove generacije 179
7.4.4 Sveobuhvatna zaštita 179
7.4.4.1 Zaštita na aplikativnom nivou 181
7.4.4.2 Zaštita na transportnom nivou 182
7.4.4.3 Zaštita na mrežnom nivou 182

7.5 Reaktivna i prediktivna zaštita 183
7.5.1 Koncept sistema reaktivne zaštite 183
7.5.1.1 Funkcionalni model reaktivne zaštite 183
7.5.1.2 Funkcionalni model reaktivne zaštite 184
7.5.2 Koncept sistema proaktivne zaštite 185
7.5.2.1 Funkcionalni model proaktivne zaštite 185
7.5.3 Organizacione mere zaštite 186
7.5.3.1 Politika bezbednosti informacionih sistema 186
7.5.3.2 Procena rizika 187
7.5.3.3 Identifikacija resursa 187
7.5.3.4 Podela resursa 188
7.5.3.5 Bezbednosne mere za zaposlene 188

8. Kriptografija 190

8.1 Osnovni kriptografski pojmovi 190

8.2 Šifarski sistemi 191
8.2.1 Simetrični šifarski sistemi 191
8.2.1.1 DES algoritam 192
8.2.1.2 AES 198
8.2.2 Diffie-Hellman protokol za razmenu ključeva 203
8.2.3 Asimetrični šifarski sistemi 205
8.2.3.1 RSA algoritam 206

8.2.3.1.1 Definicija RSA šifarskog sistema 208
8.2.3.1.2 Implementacija RSA šifarskog sistema 210
8.2.3.1.3 Bezbednost RSA algoritma 212
8.2.3.1.4 Praktična iskustva u napadima na RSA algoritam 214
8.2.3.1.5 Standardi RSA 214
8.2.3.2 Digitalni potpis 215
8.2.4 Sertifikati i infrastruktura javnih ključeva 217
8.2.4.1 Digitalni sertifikati 217
8.2.4.2 Infrastruktura javnih ključeva 218

8.3 Upravljanje ključevima 219
8.3.1 Generisanje ključa 220
8.3.2 Distribucija ključeva 221
8.3.3 Korišćenje ključeva 222
8.3.4 Skladištenje ključeva 223
8.3.5 Zamena ključa 223
8.3.6 Uništavanje ključa 224

9. Studija slučaja: Kriptografska rešenja zaštite projektovanog integrisanog automatizovanog sistema upravljanja memorije organizacije 225

9.1 Uvod 225

9.2 Profilisanje sertifikata koji će se upotrebljavati u PKI sistemu 227

9.3 Upotreba korporativnih identifikacionih kartica u informacionom sistemu 228

9.4 Višeslojna arhitektura zaštite komunikacionih kanala u okviru informacionog sistema kompanije 229

9.5 Jaka kontrola pristupa i mehanizmi zaštite informacionog sistema kompanije 231
9.5.1 Predlog rešenja jake kontrole pristupa 232
9.5.2 Konkretni predlozi potencijalnog rešenja realizacije sistema zaštite informacionog sistema kompanije 233
9.5.3 Neki mehanizmi zaštita baza podataka i sprečavanja curenja podataka iz analitičkih sistema 235
9.5.4 Kritički osvrt na predloženo rešenje i smernice za dalja istraživanja 235
9.5.5 Hipotetičko rešenje datog problema 237

10. Zaključak 242

Literatura 246

Spisak slika 282

Spisak tabela 284

1. Uvod

U praksi, kompanije često dozvoljavaju da budu opterećene ogromnom količinom informacija što je često doprinosilo haosu koji već okružuje moderne korporacije. Kako bi se ovladalo tim haosom, kompanije će imati potrebu da pronađu i suštinu načina kojim se upravlja znanjem. Svoje težište silom prilika moraće da se stave na usavršavanje načina na koji pristupaju znanju, načina kojim ga razmenjuju, na koji upravljaju, i što je najvažnije, načina na koji će ga štititi kako bi pomoću njega mogli da poboljšaju odlučivanje i omoguće efikasnije poslovanje.

Poslovanje u savremenom svetu biznisa nalazi se u okruženju velikog stepena nesigurnosti i nemogućnosti predviđanja budućnosti. Moderne kompanije suočene su sa oštrom konkurencijom, tako da su prinuđene da u potpunosti koriste sva svoja dobra od kojih je najdragoceniji znanje tj. intelektualni kapital.

Koncept poslovne inteligencije neizostavan je kada je u pitanju menadžment znanja i omogućava efikasnost u rešavanju raznih problema. Novine, pa i primena koncepta poslovne inteligencije, predstavlja izazov u kompanijama, a posebno u državnim institucijama (internim strukturama). Kompanije koje su shvatile potrebu distribucije informacija kroz organizaciju, primenjuju raznovrsne tehnike za operativno upravljanje tokovima znanja. Glavni zadatak je da povežu ljude sa sistemom koji se koristi za podelu i prenos znanja. Takođe, kompanije su otkrile da to često može da bude i veoma skupo, neefikasno i neproduktivno. Pažnja je kompletmo usmerena na uticaj informacione tehnologije i potrebu da se prema tome projektuje i sama organizaciona struktura. Upravo na ovom polju to kvalitetno rešenje, predstavljaju inteligentni sistemi za integrisano automatizovano upravljanje memorije organizacije. Zahvaljujući dostignućima koja se koriste u ovoj oblasti, mogu se prevazići određene razlike u metodskom pristupu problemu kakav predstavlja shvatanje memorije organizacije (kompletno znanje jedne organizacije – kompanije). U tom slučaju, svakako bi se poboljšalo razumevanje i omogućio novi pristup u integrisanju memorije organizacije kao važnog faktora u procesu poslovnog odlučivanja, a što bi i njenu upotrebljivost moglo da podigne na znatno viši nivo.

Integrisano automatizovano upravljanje memorijom organizacije, iako veoma složeno, predstavlja pogodno rešenje za interakciju menadžmenta znanja i informacione tehnologije. Time se stvara mogućnost potpunog objašnjavanja procesa donošenja odluka u jednoj kompaniji, ali i procesa toka dokumenata, informacija i podataka u njoj. Integrisanim, automatizovanim upravljanjem memorijom organizacije, kompanija ostvaruje mogućnost dobijanja detaljnih izveštaja na osnovu kojih je olakšano konkretno poslovno odlučivanje. Omogućava korisnicima Dalje integrisano automatizovano upravljanje memorijom organizacije omogućava korisnicima detaljniji ulazak u ovaj proces i dobijanje pomoći u analiziranju (zavisno od nivoa upravljanja) mnoštvo raznih raznovrsnih parametara.

Postavlja se i zahtev za zaštitu jednog takvog integrisanog automatizovanog procesa. U skladu sa određenim i usvojenim međunarodnim standardima (ISO 27001), menadžment u ovakvom sistemu treba reguliše sve što je vezano za proces bezbednosti informacija i njegovo upravljanje. Nameće se i potreba usaglašavanja „procesnog pristupa". Zaštita i bezbednost memorije organizacije kroz kriptografska rešenje treba da zadovolji balans između zahteva korisnika, organizacije unutar memorije i potrebu zaštite osetljivih podataka i njihov integritet. Funkcije bi trebalo da omoguće integrisani sistem upravljanja memorijom organizacije kroz sve faze koje čini poslovni proces i rad sa

dokumentima, ali i digitalno potpisivanje i kontrolu pristupa, kao i notifikaciju u sistemu. Jedan od predloženog načina rešenja zaštite integrisanog sistem za proces upravljanja memorijom organizacije u ovom radu, biće i snimanje šifrovanih dokumenata, što će omogućiti dostupnost tih podataka jedino kroz informacioni sistem kompanije. Dokumentima i podacima bi pristupali jedino ovlašćeni korisnici koji imali dozvole pristupa. Digitalnim potpisom bi se obeznedila neporecivost dokumenata, što predložena kriptografska rešenja obezbeđuju u skladu sa aktuelnim zakonskim propisima za elektronski dokument. Ovakav integrisani automatizovani proces upravljanja memorijom organizacije predstavlja jedno rešenje koje bi svoju upotrebu moglo da nađe kako u oblasti učenja inteligentnih sistema, tako i u postojećim sistemima savremenog poslovnog odlučivanja.

U radu će se razmatrati i poznati sistemi deljenja tajni, Shamirovi protokoli, tzv. „curenje" informacija itd. U razmatranju se uvek polazi od rizika u poslovanju. U ovoj doktorskoj disertaciji razmotriti će se principi i modeli koji obezbeđuju i zaštitu podataka i privilegovan pristup podacima, a sve s ciljem donošenja odluka zasnovanih na znanju koje se može podvesti pod termin memorija organizacije (korporativna memorija). Ovakvo znanje se ne može izgubiti, njime se upravlja, podaci su sigurni (nekompromitovani), u podatke se veruje, a proces donošenja odluka je takav da se uvažavaju sve prethodne odluke i iskustva i sl. Podaci, informacije i odluke su klasifikovane od najviših (strategijskih) do onih koji se svakodnevno koriste u radu (neklasifikovani podaci, slobodan pristup). Najbolji primer za ovakvu analizu su bezbednosno-informativne agencije, a brojni su primeri, kako dobrih organizacija, tako i propusta u njihovom radu (Snouden, Asanž…).

1.1 Metodološke osnove istraživanja

Problem ovog istraživanju sadržan je u segmentu bezbednosti, koji se bavi kriptografskim rešenjima zaštite memorije organizacije sa stanovišta menadžmenta znanja, s ciljem očuvanja poverljivosti, integriteta i dostupnosti resursa memorije organizacije u sistemu odlučivanja u modernim kompanijama. Sama kompleksnost predmeta istraživanja i opširnost materije tri segmenta: kriptografske zaštite, memorija organizacije i upravljanje znanjem, definisanost problema istraživanja može se predstaviti primenom odgovarajućih matematičkih i statističkih metoda, kao i metoda mašinskog učenja.

1.1.1 Predmet i cilj istraživanja

Predmet istraživanja ovog rada su kriptografska rešenja zaštite memorije organizacije sa stanovišta menadžmenta znanja. Oblast integrisanog automatizovanog procesa upravljanja znanjem zauzima sve važnije mesto u savremenom poslovnom okruženju. Znanje jedne organizacije – kompanije predstvlja ključni resurs. Zaštita i bezbednost tog znanja je od ključnog značaja za opstanak jedne organizacije – kompanije.

Napor da se znanje jedne kompanije organizuje, da se usaglasi upravljanje procesima poslovnog odlučivanja doveli su do razvoja integrisanog automatizovanog procesa upravljanja znanjem. Količina znanja koja nam je dostupna i od interesa, da ukoliko ne postoji dobar način da njime upravljamo, nećemo moći ni da ga efektivno i efikasno koristimo.

Uspešna implementacija programa menadžmenta znanja u memoriji organizacije predstavlja kompleksan postupak koji zahteva poštovanje balansa između ljudskog faktora i informacionih tehnologija. Samim tim, sistem upravljanja znanjem jedne kompanije mora

da potvrdi svoju ulogu u smislu dostavljanja potrebnih podataka do zaposlenih u kompaniji na osnovu kojih će se proveriti sve opcije i doneti konačna odluka koja će biti prosleđena u daljem procesu poslovnog odlučivanja i vođenja same kompanije. Uvođenjem integrisanog automatizovanog procesa upravljanja znanjem u kompaniji postiže se povećanje vrednosti kompanije i obezbeđuje se donošenje brzih i efikasnih odluka..

Kontradikcija između potrebe za povećanjem brzine i fleksibilnosti reakcije informacione tehnologije, istovremenog nastojanja smanjenja opterećenja skladištenja i obezbeđivanja kontrole, zaštite i bezbednosti znanja kod mnogih kompanija stvara kompleksnu i opterećenu IT infrastrukturu. Samim tim, neophodna su organizovana mesta skladišta podataka uz uspostavljanje integrisanog automatizovanog procesa upravljanja i zaštite bezbednosti tih podataka. Ovim bi se pojednostavila administracija, uz istovremeno povećanje fleksibilnosti administratora za upravljanje znanjem u kompaniji. Potreban je pristup da sama infrastruktura integrisanog automatizovanog procesa upravljanja memorijom organizacije bude, usaglašena sa određenim međunarodnim standardima (ISO 27001) i da omogućava efikasno korišćenje sistema.

Integrisano automatizovano upravljanje memorijom organizacije, iako veoma složeno, predstavlja pogodno rešenje za interakciju menadžmenta znanja i informacione tehnologije čime se stvara mogućnost potpunog objašnjavanja procesa kako donošenja odluka u kompaniji, tako i procesa toka dokumenata, informacija i podataka u njoj. Takođe, omogućava da korisnici detaljnije uđu u ovaj proces i dobiju pomoć u analiziranju (zavisno od nivoa upravljanja) mnoštva raznih parametara. Praktično, nakon proučavanja parametara, sagledavanja problema, međusobnih konsultacija i interakcija sa postojećim iskustvom (znanjima o određenim okolnostima i pojavama koja se već nalaze u organizacionoj memoriji) konačno se dolazi do ispravnog poslovnog odlučivanja.

Zahvaljujući dostignućima koja se koriste u ovoj oblasti, mogu se prevazići određene razlike u metodološkom pristupu problemu kakav predstavlja shvatanje memorije organizacije. Time bi se svakako poboljšalo razumevanje i omogućio novi pristup u integrisanju memorije organizacije kao važnog faktora u procesu poslovnog odlučivanja, a što bi upotrebljivost memorije organizacije svakako moglo da podigne na znatno viši nivo.

Logički se nameće i zahtev za zaštitu jednog takvog integrisanog automatizovanog procesa. Menadžment u ovakvom sistemu treba da obezbedi kompaniji, u skladu sa određenim i usvojenim međunarodnim standardima (ISO 27001), usaglašavanje „procesnog pristupa" primenom sistema procesa u organizaciji, zajedno sa identifikovanjem i međusobnom interakcijom procesa i njihovim upravljanjem.

U ovoj doktorskoj disertaciji, biće predstavljena i predložena kriptografska rešenja u zaštiti memorije organizacije sa stanovišta menadžmenta znanja. Ovakav integrisani automatizovani proces posebno je koristan u objašnjavanju složenih poslovnih situacija koje se mogu javiti u praksi svake moderne kompanije. Sistem omogućava razmenu informacija korisnika sistema, zajedno sa čuvanjem istorije događaja u sistemu. Pored toga, pruža i efikasnu razmenu informacija između korisnika sistema putem definisanih radnih procedura, tj. definisanih tokova informacija u poslovnom sistemu, čime se obezbeđuje uspešno nadgledanje događaja u sistemu. Efikasno praćenje radnih operacija, obezbeđuje se čuvanjem kompletne istorije događaja. Njihovom razmenom sa okolinom, kao i implementacijom definisanih poslovnih procedura olakšava se definisanje radnih zadataka učesnika u okviru sistema. U tom pogledu, od velike pomoći je i primena arhiviranja dokumenata o poslovanju. Upotreba integrisanog sistema za proces upravljanja memorijom organizacije kompletna arhivska građa kompanije postaje centralizovana, lako dostupna i organizovana.

Tema doktorske disertacije su upravo kriptografska rešenja zaštite jednog softverskog sistema integrisanog automatskog procesa upravljanja memorijom organizacije sa stanovišta menadžmenta znanja. Zaštita i bezbednost memorije organizacije kroz kriptografska rešenja trebaju da zadovolje balans između zahteva korisnika, projektovanja memorije organizacije, potrebe zaštite osetljivih podataka i njihov integritet. Osnovne karakteristike takvog sistema su: upravljanje fizičkim čuvanjem dokumenata; logička organizacija dokumenata; upravljanje njihovim životnim ciklusom; akcije za rad sa dokumentima; digitalizacija tekuće dokumentacije; pretraživanje dokumentacije; digitalno potpisivanje dokumenata; kontrola pristupa dokumentima; arhiviranje dokumenata; podrška za rad više učesnika; podrška za definisanje poslovnih procesa (*workflow*); procedure za automatsko vođenje poslovnih procesa; beleženje svih događaja u radu sa dokumentima; notifikacija o događajima u sistemu. Jedan od predloženog načina zaštite integrisanog sistema za proces upravljanja memorijom organizacije je i mogućnost njihovog snimanja u kriptovanom obliku, čime podaci postaju dostupni samo kroz sistem. Pristup dokumentu bi imali samo ovlašćeni korisnici sistema. Autentičnost dokumenata i njihova nepromenljivost će se obezbediti digitalnim potpisivanjem, što je u skladu sa aktuelnim zakonskim propisima za elektronski dokument. Ovakav predlog kriptografske zaštite integrisanog automatizovanog procesa upravljanja memorijom organizacije predstavlja rešenje koje bi svoju upotrebu moglo da nađe kako u oblasti učenja inteligentnih sistema, tako i u postojećim sistemima savremenog poslovnog odlučivanja.

Osnovni cilj istraživanja koje će biti sprovedeno tokom rada, je da se na osnovu šire literature sagleda problem rešenja kriptografske zaštite memorije organizacije sa stanovišta menadžmenta znanja, kao i to da se istraži mogućnost formalizacije i integrisane automatizacije memorije organizacije sa stanovišta mendžmenta znanja.

Posebni ciljevi doktorske disertacije su:

- ispitati mogućnost formalizacije i integrisane automatizacije eksplicitnog i implicitnog znanja jedne organizacije – kompanije u delu prikupljanja podataka, obrade i učitavanja podataka iz operativne baze memorije organizacije (skladišta podataka),
- istražiti mogućnost uticaja formalizacije i digitalizacije memorije organizacije na kvalitet dizajna i brzinu dobijanja informacija o poslovnim procesima i potrebama korisnika za informacijama,
- dokazati upotrebnu vrednost automatizacije memorije organizacije, kroz obezbeđivanje njene zaštite i olakšavanja pristupa, deljenja podataka i informacija i njeno ponovno korišćenje kroz integrisani automatizovani proces upravljanja znanjem,
- istražiti mogućnost primene kriptografske zaštite integrisanog automatizovanog procesa za upravljanje memorije organizacije u oblasti poslovnog odlučivanja, kroz elektronsko upravljanje podacima prilagođeno korisničkom nivou,
- istražiti mogućnosti kriptografskih rešenja zaštite memorije organizacije sa stanovišta menadžmenta znanja, sa težištem na očuvanje poverljivosti, integriteta i dostupnosti resursa memorije organizacije u procesu poslovnog odlučivanja u modernim kompanijama,
- predlog kriptografskog rešenja u zaštiti integrisanog automatizovanog procesa upravljanja memorijom organizacije, koji bi nadomestio nedostatke prikazanih rešenja i uveo određene nove koncepte i smernice za dalji rad.

1.1.2 Istraživačke hipoteze

U okviru ove doktorske disertacije postavljena je sledeća osnovna hipoteza sa preliminarnim i teoretskim određenjem predmeta istraživanja:

H0: Kriptografska zaštita integrisanog automatizovanog procesa upravljanja memorijom organizacije osnovni je preduslov za efikasno učenje, ali i brže i sadržajnije poslovno odlučivanje kompanije koja ga koristi.

Iz osnovne hipoteze izvode se sledeće posebne hipoteze koje obrađuju delove predmeta istraživanja:

H1: Uspešnost kompanije i njenih poslovnih rezultata direktno zavisi od efikasnosti zaposlenih, međusobnim deljenjem znanja;

H2: Memorija organizacije je jedna od najvažnijih organizacijskih elemenata koju kompanija ima, tako da je potrebno projektovati načine da sadržaji memorije budu dostupni svima u kompaniji (prema nivoima odlučivanja) i da se ista adekvatno i efikasno zaštiti;

H3: Integrisano automatizovani proces upravljanja memorijom organizacije omogućava evidenciju podataka o dokumentima, elektronsko upravljanje dokumentacijom iz poslovnog sistema, upravljanje definisanim procedurama za rad sa poslovnim dokumentima ili predmetima (skupovima dokumenata);

H4: Korišćenjem integrisanog automatizovanog procesa upravljanja memorijom organizacije 94alizuje se politika sigurnosti, sistem upravljanja kvalitetom, sigurnost zaposlenih, sigurnost materijalnih dobara i životne sredine, operativno upravljanje i komunikacija i upravljanje kontinuitetom poslovanja čime se doprinosi povećanju kvaliteta i efikasnosti poslovnog odlučivanja;

H5: Zaštitom integrisanog automatizovanog procesa upravljanja memorijom organizacij97nora se obezbediti visok nivo sigurnosti i zaštite svih dokumenta putem definisanja prava i ograničenja pristupa na nivou pojedinačnih korisnika ili grupa korisnika paralelno sa integrisanim programom za upravljanje dokumentima u memoriji.

1.1.3 Metode istraživanja i tok istraživačkog postupka

Metodologija istraživanja u okviru ove doktorske disertacije sadrži složen pristup 48i se sastoji od logičkih načela i principa po definisanim fazama. Polazna metoda istraživanja prilikom izrade doktorske disertacije bila je prikupljanje i proučavanje dostupnih izvora literature, njihova analiza i sistematizacija, a sve u cilju ukazivanja na opravdanost i korisnost razvoja kriptografske zaštite memorije organizacije sa stanovišta menadžmenta znanja.

Za izradu doktorske disertacije osim opštih naučnih metoda, korišćene su i metode modelovanja i analitičko-deduktivna tehnika. Metoda modelovanja je upotrebljena 48likom definisanja modela memorije organizacije, implementacije kriptografskih rešenja i praktične provere rezultata istraživanja. Kod analize podataka o postojećim rešenjima u oblasti menadžmenta znanja kriptografske zaštite i skladištenja podataka korišćena je analitičko-deduktivna tehnika, odnosno metoda. Osim navedenih metoda, prilikom definisanja modela memorije organizacije, korišćeni su i posebni metodološki postupci kao što su generalizacija (definicija generičkog tipa) i specijalizacija kao inverzni postupak (definisanje specifičnih osobina nekih objekata).

Istraživanje je sprovedeno kroz nekoliko faza. U okviru prve faze je prikupljena i proučena dostupna literaturža u oblasti projektovanja memorije organizacije, menadžmenta znanja i kriptografskih rešenja, njena analiza i sistematizacija, sa akcentom na

automatizaciji projektovanja memorije organizacije sa stanovišta menadžmenta znanja i implementaciji kriptografske zaštite. Identifikovani su i kategorizovani postojeći pristupi. Naredna faza istraživanja bila je proučavanje memorije organizacije (na principu *Data Warehouse*), analiza njenih prednosti i nedostataka. Glavni deo istraživanja odnosio se na formalizaciju upravljanja memorijom organizacije u svrhu principijelnog upravljanja fizičkim skladištenjem dokumenata; njihovom organizacijom u logičke strukture; upravljanju životnim ciklusom; akcijama za rad sa dokumentima; digitalizacijom; pretraživanjem; digitalnom potpisivanju dokumenata; kontroli pristupa; arhiviranju dokumenata; podršci za kolaboraciju više učesnika; podršci za definisanje poslovnih procesa (*workflow*); automatskim procedurama za vođenje poslovnih procesa; beleženju svih događaja u radu sa dokumentima, kao i notifikaciji o događajima u sistemu. Poseban akcenat dat je i na zaštiti integrisanog sistema za upravljanje memorijom organizacije kroz ispitivanje mogućnosti snimanja dokumenata u šifrovanom obliku, čime su podaci postali dostupni isključivo kroz sistem, dok je pristup dokumentima garantovan samo korisnicima sistema koji su za to eksplicitno ovlašćeni preko definisanih dozvola pristupa.

U poslednjoj fazi istraživanja implementirana je kriptografska zaštita u memoriji organizacije zasnovane na menadžmentu znanja i demonstrirana je upotrebna vrednost rezultata istraživanja na praktičnom primeru modela jedne organizacije.

Ovakav izbor metoda istraživanja je korišćen u svrhu korektnog izvođenja istraživanja i toka istraživačkog procesa u svim fazama, odnosno identifikaciji i formulaciji problema, planiranju dizajna istraživanja, prikupljanju, obradi i analizi podataka, kao i definisanju zaključaka u skladu sa osnovnim načelima naučnoistraživačkog rada. Svi metodološki postupci su podjednako zastupljeni, čime se ostvaruje integrativan i sintetički pristup istraživanju.

1.2 Očekivani rezultati istraživanja i naučni doprinos

Svrha ovog rada je da informiše stručnjake u oblasti informcionih tehnologija o značaju i pravilnim načinima implementacije integrisanog automatizovanog upravljanja u memoriji organizacije baziranoj na menadžmentu znanja. Odnosno, predlogom kriptografske zaštite memorije organizacije sa stanovišta menadžmenta znanja, čime bi se značajno povećala bezbednost komunikacije unutar memorije organizacije i ujedno izvršilo poboljšanje performansi za upravljanje i zaštitu dokumenata, kroz integraciju sistema organizovanja dokumenata, pretraživanja, analizu, čuvanje, i hijerarhijsko upravljanje dokumentima u memoriji organizacije.

U ovoj disertaciji očekivani su sledeći stručni doprinosi:

- Potenciranje važnosti zaštite i upotrebe svih dostupnih mogućnosti koje pruža memorija organizacije zasnovana na menadžmentu znanja u jednoj kompaniji.
- Pregled tehnologija, alata, softverskih rešenja i vodećih baza podataka koje se mogu pogodno koristiti za razvoj i unapređenje memorije organizacije kroz integrisano automatizovano upravljanje.
- Pregled međunarodnih standarda za bezbednost informacija kroz definisanu poverljivost, integritet i pristup informacijama u kompaniji.
- Razvoj kriptografskih rešenja zaštite integrisanog automatizovanog procesa upravljanja memorije organizacije zasnovane na menadžmentu znanja, kroz rešenja za upravljanje i zaštitu dokumenata, kroz integraciju sistema organizovanja dokumenata, pretraživanja, analize, čuvanja, i hijerarhijskog

upravljanja dokumentima.

- Analiza primera korišćenja standardne metodologije i alata za softversko modelovanje za implementiranje otvorenih standarda i omogućavanje njihove integracije sa drugim aplikativnim rešenjima za poslovno odlučivanje.

Integrisanom automatizovanom upravljanju memorijom organizacije baziranom na menadžmentu znanja pripada veoma značajno mesto u određivanju strategijske prednosti kompanija na tržištu. Upravljanjem memorijom organizacije i njenom adekvatnom kriptografskom zaštitom obezbeđuje se veća efikasnost i produktivnost, bezbednost na svim nivoima unutar kompanije, efektivnost, bolja iskorišćenost radnog vremena, produktivnost i sigurnost komunikacija, efikasna organizacija, uređenost arhive, manji broj izvršilaca u poslovnom procesu, manji troškovi, ali pre svega postiže se konkurentnost prema drugim kompanijama.

Naučna opravdanost ovog istraživanja leži u sve većoj potrebi da se izvrši jedan pregled, analiza i klasifikacija postojećih rešenja u zaštiti integrisanog automatizovanog sistema upravljanja memorije organizacije, kao najznačajnijeg resursa svake kompanije.

Naučni doprinosi:

- Poboljšanje nivoa zaštite integrisanog automatizovanog procesa upravljanja memorije organizacije u savremenom poslovnom odlučivanju, kroz pregled, analizu, klasifikaciju i kriptografsku zaštitu svih segmenata organizacije u skladu sa savremenim zahtevima poslovanja.
- Realizacija kriptografskih rešenja zaštite integrisanog automatizovanog upravljanja memorijom organizacije, kojim bi se obezbedila jedinstvena sredina za rad sa dokumentima, kao i brz, kontrolisan i bezbedan pristup na svim nivoima.
- Predlog smernica za dalji razvoj pristupa kriptografskoj zaštiti integrisanog automatizovanog upravljanja memorijom organizacije na bazi menadžmenta znanja.
- Rezultati rada disertacije su objavljeni u relevantnim međunarodnim časopisima i saopšteni na naučnim skupovima u zemlji i inostranstvu.

1.3 Pregled sadržaja po poglavljima

Disertacija je realizovana u devet poglavlja i to prema sledećem.

U uvodnom poglavlju, daje se kratak prikaz sveobuhvatnog poduhvata i svih izazova istraživanja, kroz uvod u područje i problema koji se istražuje. Definiše se predmet i cilj istraživanja, daje se pregled dosadašnjih rezultata u ovoj oblasti, zatim polazne hipoteze, osvrt na metode istraživanja kao, i očekivani naučni i stručni doprinos rezultata istraživanja.

Poglavlje 2 posvećeno je teoriji znanja i razmatrano je opšte stanje u oblasti istraživanja. Opisane se razlike značenja podatka, informacije i znanja kao i kategorizacija znanja uz konsultovanje različitih izvora i teorija. U nastavku poglavlja opisane su strategije upravljanja zanjem kroz opis generičke i opšte strategije uz objašnjenje elementa strategije upravljanja znanjem i savete kako i na koji način izgraditi strategiju menadžmenta znanja. Poglavlje se završava elaboriranjem ekonomije znanja kroz prednosti primene i pepreke i poteškoća u menadžmentu znanja.

Poglavlje 3 bavi se teorijskim osnovama istraživanja menadžmenta znanja kao jedne od tri celine istraživanja u ovoj doktorskoj tezi. Analizirane su definicije menadžmenta znanja i objašnjena suština samog koncepta menadžmenta znanja. Poseban osvrt u ovom delu disertacije posvećen je intelektualnom kapitalu, menadžmentu znanja i znanju kao nevidljivoj imovini svake kompanije. Uvidom u veći broj naučnih radova koji obrađuje ovu problematiku, analizirani su elementi i modeli menadžmenta znanja kao i implementacija menadžmenta znanja u praksi. U završnom delu ovog poglavlja objašnjene su tehnologije i alati menadžmenta znanja i predstavljene perspektive primene koncepta menadžmenta znanja u praksi u budućnosti.

Poglavlje 4 usredsređeno je na konceptualnu tehnološku infrastrukturu kompanije kao celinu koja je preduslov za razvijanje informacionih sistema i kreiranje znanja u kompanijama. Dat je kritički osvrt na proces reinženjeringa u kompanijama kroz analizu uvođenja savremenih organizacionih struktura, procesnog pristupa i razvoj informacionih sistema u kompanijama koji pre svega treba da služi automatizaciji i integraciji proizvodnih i poslovnih procesa sa jedne strane, kao i da predstavlja glavnu komunikacionu osnovu između pojedinih organizacionih celina u kompanijama. Poseban osvrt posvećen je sistemima za podršku u odlučivanju, ekspertnim sistemima, sistemima za menadžment dokumentima i informacionim sistemima za kreiranje znanja. Poglavlje se završava analizom koncepta organizacije koja uči, jer u savremenoj i digitalizovanoj ekonomiji, efikasno korišćenje znanja predstavlja najizdašniji i postojan izvor konkurentske prednosti svake kompanije. I na kraju, kritički se određujemo prema sistemu poslovne inteligencije jer on u sebi sadrži elemente strategije, poslovne analize, marketinga i informacione tehnologije kako bi se izvršilo prikupljanje, analiza, distribucija i delovanje na osnovu dobijenih poslovnih informacija, radi lakšeg upravljanja i donošenja najboljih poslovnih odluka u kompanijama.

Poglavlje 5 posvećeno je rudarenju podataka, jer kao takvo tretira važnost i ulogu otkrivanja znanja u poslovnoj inteligenciji svake kompanije. Dat je kratak pojam rudarenja podataka kroz zadatke – probleme rudarenja podataka. Predstavljen je odnos rudarenja podataka i otkrivanja znanja kroz kritički osvrt i analizu koraka u procesu otkrivanja znanja. Pored toga, analizirana je priprema podataka za rudarenje kroz procesuiranje, analiza relevantnih atributa i završni postupci. Poseban akcenat stavljen je na tehnike rudarenja podataka u kome su kritički razmatrane metoda regresije, klasifikacione metode, metode klasterovanja, neuronske mreže, stablo odlučivanja, metode za analizu veza i genetski algoritmi. Ovo poglavlje disertacije završava se kroz zaključno predstavljanje načina na koji se koristi znanje koje je otkriveno u procesu rudarenja podataka i predstavlaju se područja u kojima je moguća primena alata za rudarenje podataka.

Poglavlje 6 predstavlja drugu celinu disertacije i obrađuje memoriju organizacije kao fenomen i potrebu svake kompanije koja želi da uspostavi sisteme poslovne inteligencije i osvoji svoju konkurentnost na međunarodnom tržištu. Date su kritičke osnove definicije memorije organizacije. Predstavljene su tipologije i informatičke pretpostavke prilikom formiranja memorije organizacije koja bi u zavisnosti od svojih potrebnih funkcija bazirala na dokumentima, na menadžmentu znanja, bila zasnovana na slučajevima, ili pak bila distribuirana ili predstavljala kombinaciju raznih drugih tehnika. Poseban kritički osvrt stavljen je na probleme upravljanja sa velikom količinom podataka, a što se odnosi na: Big Data sisteme, sisteme za planiranje poslovnih resursa – ERP sisteme, Data Warehouse sisteme, Računarstvo u oblaku – Cloud Computing i Hadoop sisteme, jer korist iz tekuće digitalne revolucije izvlače samo one kompanije koje su sposobne da efikasno upravljaju podacima i da na osnovu njih donesu zaključke koji vode efikasnim poslovnim odlukama.

Poglavlje 7 predstavlja uvod u treću celinu i posvećeno je optimizaciji zaštite memorije organizacije. Najpre je razmatrano opšte stanje u oblasti istraživanja kroz analizu pretnji i ranjivosti memorije organizacije uz objašnjenje sofistikacije malvera i raznih vrsta napada. Završni deo ovog poglavlja disertacije analizira zaštitu kontejner tipa kroz opis antivirusne i firewall zaštite, odnosno daje pregled koncepata IDS/IPS sistema i slojevite zaštite. Objašnjene su faze reagovanja na napad i dat je pregled sistema za sprečavanje upada. U završnom delu poglavlja kritički su analizirani koncept sistema reaktivne i proaktivne zaštite i predložene su organizacione mere zaštite kroz politiku bezbednosti informacija, procenu rizika, identifikaciju resursa i bezbednosnih mera za zaposlene.

Poglavlje 8 posvećeno je kriptografiji i logički je nastavak treće celine disertacije koji obrazlaže teorijske osnove istraživanja. Uvidom u veliki broj naučnih radova, navedene su prepoznate prednosti osnovnih šifarskih sistema, kao i njihov značaj na polu zaštite privatnosti i informacija. Predstavljeni su simetrični i asimetrični šifarski sistemi, kao i Diffie-Hellman protokol za razmenu ključeva. Poseban osvrt dat je na digitalnom potpisu i upravljanju ključevima. Osim već poznatih rezultata na polju zaštite privatnosti, kriptografska rešenja daju nam i nove ideje o mogućnostima upravljanja ključevima. Razmatraju se i novi principi kao i pristupi u okviru servisa za autentifikaciju, naročito u segmentu odvojene optimizacije pojedinih podsistema u kompanijama.

Poglavlje 9 kritički analizira studiju slučaja kriptografskog rešenja zaštite projektovanog integrisanog automatizovanog sistema upravljanja memorije organizacije. Predstavljena je studija slučaja, sa osvrtom na jedan hipotetički pristup sa aspekta jake kontrole pristupa i višeslojne arhitekture zaštite memorije organizacije. Skup podataka i metodologija istraživanja u ovoj studiji slučaja dovodi do profilisanja sertifikata koji će se upotrebljavati u PKI sistemu. Vrši se izdvajanje atributa koji regulišu upotrebu korporativnih identifikacionih kartica u informacionom sistemu kompanije. Predlaže se višeslojna arhitektura zaštite komunikacionih kanala u okviru informacionog sistema kompanije u korišćenju resursa memorije organizacije. Predložen je testiran model jake kontrole pristupa i mehanizmi zaštite informacionog sistema – memorije organizacije koja obuhvata mehanizme zaštite baza podataka i sprečava curenje podataka iz analitičkih sistema. Na kraju, dat je kritički osvrt na rešenje i predložene su smernice za eventualna dalja istraživanja. .

U završnom poglavlju disertacije dat je zaključak. Sumirani su svi ciljevi koji su postavljeni na početku istraživanja. Predstavljeni su i ostvareni rezultati i doprinosi u radu. Izvršeno je razmatranje moguće oblasti u kojima se predloženo rešenje kriptografske zaštite može primeniti. Kao osnovne oblasti primene identifikovani su većina kriptosistema koji egzistiraju u kompanijama, prvenstveno oni sistemi koji su od velike važnosti za informacionu bezbednost kako velikih kompanija, tako i državnih institucija.

2. Teorija znanja

Neizvesnost u savremenom načinu poslovanja predstavlja dominantnu karakteristiku poslovnog okruženja [1], što implicira da je od presudne važnosti za opstanak i uspeh svake kompanije na tržištu njena sposobnost da prikupi [2], analizira i procesira, [3] svaki izvor podataka na drugačiji način [4].

Znanje sada predstavlja važan resurs kompanije i njegov značaj je naročito naglašen u savremenom poslovanju. U koncipiranju strategije tehnološkog razvoja doprinos naučnika je neizostavan, a naročito onda kada su evidentno proizvedeni i neprekidno se proizvode i razvijaju ogromni fondovi znanja.

2.1 Podatak, informacija, znanje

Kako bi se razumeo pojam menadžment znanja potrebno je najpre razumeti kako razlikovati znanje od podatka ili informacija. U svemu tome otežava i činjenica da ne postoji jedna univerzalna i opšte prihvaćena definicija znanja. Na naučnom nivou nije postignut konsenzus o tome šta se tačno podrazumeva kada je u pitanju znanje, onosno gde je granica znanja u odnosu na neke bliske kategorije kao što su podatak, informacija i mudrost.

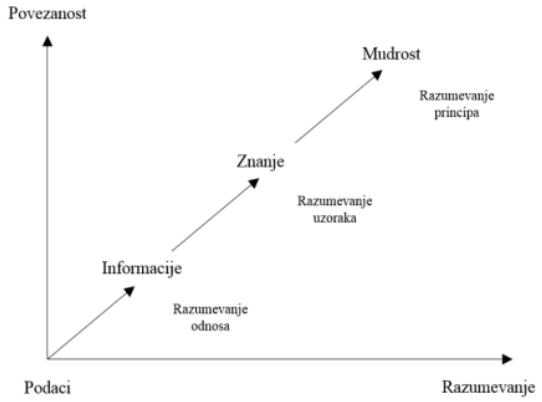
Podatak (engl. *data*) se može definisati kao *skup odvojenih, objektivnih činjenica o nekom događaju*.[5] Podatak opisuje samo deo događaja (pojave), ne omogućava donošenje stava (suda) ili objašnjenje nekog događaja. Podaci, u osnovi, daju samo kvantitativni prikaz događaja, ali ne i odgovore na pitanja: Zašto se desio neki događaj? Koje su bile posledice? Hoće li se događaj ponoviti?... On predstavlja opažanje, sirovu činjenicu ili činjenicu van konteksta; on je nestruktuirani (nesređeni) zapis u obliku brojeva, teksta, slike ili kombinacije svega, koji sam za sebe, nema neku posebnu vrednost. Kada se odgovarajućom obradom podacima da značenje, svrha i relevantnost, oni postaju informacije koje mogu biti korisne za poslovno odlučivanje ili delovanje. Koskineni i Pihlanto daju definiciju podataka kao neobrađenih činjenica, kao što su brojevi i slova sa dodatkom konteksta kako bi mogla nastati informacija.[6] Saaristo u svojim istraživanjima tvrdi da kombinujući informaciju sa postojećim uverenjima, veštinama i percepcijom pojedinca nastaje znanje. Samim tim, podaci, informacije i znanje su posebni entiteti.[7]

Termin informacija (od lat. *Informare* – formirati stav) mogao bi da se definiše kao poruka, najčešće u pisanom obliku ili lična komunikacija, koja ima svog pošiljaoca i primaoca.[5]. Informacija predstavlja rezultat obrade podatka i ima osobinu da otklanja neku neizvesnost i pomaže u poslovnom odlučivanju i ima neko značenje.[8] Prilikom organizacionog dizajniranja kompanije ključni izazov predstavlja usklađivanje potrebe za procesuiranjem informacija sa kapacitetom kompanije za njihovo procesuiranje.9] Ovo se posebno može uočiti kod kompanija kod kojih je kapacitet procesuiranja informacija manji od potrebnog.[10] Kompanija koja je svesna vrednosti podataka i informacija, i upravlja njima na odgovarajući način, može poboljšati svoje poslovanje.[11] To čini kroz prilagođavanje postojećih i uvođenjem novih proizvoda i usluga,[12] boljim razumevanjem potreba kupaca, izbegavanjem rizika i smanjenjem troškova.[13] Tu se postavlja pitanje: *Ko odlučuje da li je nešto informacija ili je samo podatak, odnosno ima li neka poruka značenje ili ne?* Imajući u vidu da je svrha informacije (kao što se može primetiti u korenu te reči) da informiše, nameće se logičan zaključak da je primalac taj koji odlučuje da li je primljena poruka za njega informacija, odnosno da li nosi neko značenje, ili predstavlja

samo neki podatak, odnosno skup nepovezanih činjenica.

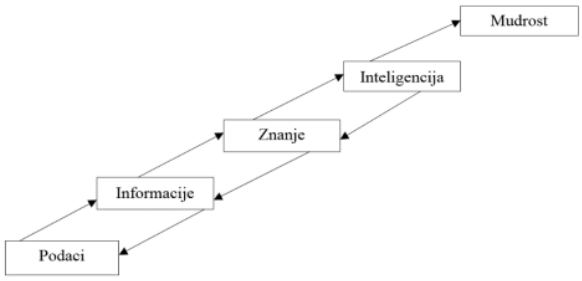
Definisanje pojma znanja je ipak zahtevnije. Saaristo [7] pak tvrdi da ni znanje a ni podaci ne predstavljaju informacije. Ipak, bez podataka i informacija ne može postojati znanje. Znanje čini skup informacija s ciljem da se ostvari njihova korist i upotrebna vrednost koje predstavljaju smernice za akciju. Znanje podrazumeva skup relevantnih informacija prikupljenih blagovremeno i na pravom mestu, dostupnih u svakom momentu po potrebi, a koje su uz to neophodne za efektivno odlučivanje i delovanje.[9] Na temelju postojećih ličnih uverenja i njihovog kombinovanja sa informacijama nastalim na osnovu podataka nastaje novo znanje. Znanje, dakle, omogućava akciju kojom se dolazi do rešenja problemskih situacija i lakše donose nove poslovne odluke.

Vrh piramide znanja je mudrost.[14] Mudrost je kategorija koja se odnosi na sposobnost pojedinca da kombinuje znanje, iskustvo i intuiciju. Mudrost je i produkt akumuliranog znanja, tj. rezultat dugoročnog procesa učenja.



Slika 1. *Hijerarhija podatak–informacija–znanje–mudrost*
Izvor: [15]

Za prihvatljivu definiciju prethodno navedenih pojmova, ukazivanje na njihove razlike i međusobne odnose u teoriji i praksi, treba primeniti hijerarhiju. Ovakva hijerarhija poznata je i pod drugim nazivima: *Hijerarhija znanja, Informaciona hijerarhija, Piramida znanja, Hijerarhija mudrosti* (slika 1).[16] Više autora, kao osnovne elemente u hijerarhijama predstavljaju – podatke, informacije i znanje[17], dok su pojedini autori u svojim istraživanjima nadogradili ovu hijerarhiju i u nju uključili inteligenciju i mudrost.[18]



Slika 2. *Hijerarhija podaci–informacije–znanje–inteligencija–mudrost*
Izvor: [18]

Podaci se nalaze na najnižem nivou hijerarhije. [18] U sirovom obliku podaci nemaju nikakvo značenje, bez obzira odakle potiču, odnosno da li su interni ili eksterni..[19] Da bi iz njih nastala informacija, treba da se organizuju i interpretiraju u odnosu na određenu situaciju [20] koja poseduje svoje značenje i konkretnu poruku. [21] Danas, informacije imaju značajno mesto u svakoj kompaniji, jer su kompanije postale visoko zavisne od njih [22] i smatra se da moć leži upravo u kontrolisanju toka informacija. [23] Podaci čine polaznu osnovu za kreiranje informacija, dok za kreiranje znanja informacije predstavljaju neophodan input. [24] Informacija koja ima kontekst predstavlja znanje i na osnovu nje mogu se preduzimati određene aktivnosti. [25] Treba istaći da znanje nastaje kroz rad i iskustvo zaposlenih, da ga je teško kodifikovati i da ne proizilazi automatski iz prikupljenih informacija. [26]

Znanje ne može opstati bez podrške informacionih tehnologija. U procesu kreiranja znanja informaciono-komunikacione tehnologije imaju veliki značaj. [27] Primenom ovih tehnologija u poslovanju kompanija mogu nastati značajne promene. [20]

Inteligencija i mudrost nalaze se na vrhu piramide znanja. Pod inteligencijom se podrazumeva sposobnost da se sagleda i razume okruženje, naprave odluke i sprovedu akcije kojima će se povećati efikasnost kompanije. [28] Efektivnost kompanije se povećava primenom mudrosti [15] koja predstavlja upravljanje događajima izvan postojećih šablona kroz primenu stečenog znanja. [29] Pored toga, pomoću nje se postiže prilagođavanje potpuno novim situacijama primenom različitih tehnika i metoda. [30]

Sumirajući navedeni prikaz i relacije prikazane u njemu može se zaključiti sledeće:

- Informacije su povezane sa opisom, definicijama i perspektivama.
- Pod znanjem se podrazumeva strategija, praksa, metode i pristupi.
- Mudrost uključuje primenu principa, pronicljivost, moral ili arhetip. [31][32]

2.1.1 Pojmovno određivanje znanja

Već smo pomenuli da pojedini autori među kojima su Meyer i Sugiyama [33] ističu da ne postoji jedna, opšte prihvaćena definicija znanja. Veliki problem leži u nepoznavanju načina kreiranja znanja. Poznato je kako *znanje potiče i koristi se unutar uma pojedinca* [5], ali kakav je tok tog proces u glavama još uvek je misterija. Međutim, kako bi se omogućio menadžment znanja, potrebno je pokušati postaviti barem radnu definiciju znanja. Davenport i Prusak [5] daju definicju znanja koja se ogleda u činjenici da je to skup organizovanih iskustava sa vrednošću informacija i razumevanja koja definišu evaluaciju novih iskustava i informacija. Po njima se znanje može definisati i kao mešavina iskustva, vrednosti i informacija koje se nalaze u okviru nekog konteksta a koje obezbeđuje procenu i korišćenje novih informacija i iskustava. [5] Za primer definicije znanja uzećemo Kermalija i Sveibija. Prema Kermaliju znanje se može ukratko definisati kao *upotreba informacija*; [34] dok Šveđanin Karl Erik Sveibi definiše znanje kao spoznaju usmerenu na akciju, baziranu na pravilima i orijentisanu ka stalnim promenama. [35]

Bitno je napomenuti da se znanje u suštini razlikuje od informacije, i samim tim zahteva različite metode za njegovo prenošenje. Tako Beveren [36] pravi razliku između podataka i informacija kao jedinih oblika poruke koji se mogu zabeležiti, prenositi ili skladištiti izvan ljudskog uma, te da znanje može egzistirati samo u umovima pojedinaca. McDermott [37] navodi šest karakteristika koje znanje razlikuju od informacije: (1) posledica je ljudskog delovanja, (2) proizlazi iz razmišljanja, (3) kreira se u realnom vremenu, (4) pripada zajednicama, (5) cirkuliše kroz zajednice na različite

načine, (6) kreira se na granici tamo gde staje staro znanje.

Alavi i Leidner tvrde, da se u svom krugu eksploatacije, neka informacija kod pojedinaca pretvara u znanje, u cilju tretiranja kao informacije kada se pretvori u tekst, grafikone, reči i tabele.[38] Dalje, Hiks, Dattero i Galup tvrde da se krug ponovo nastavlja kada se ta ista informacija, uskladištena prenese nekom pojedincu i time postane njegovo znanje.[39] Ili kako Lee i Yang[40] posmatraju taj odnos: *znanje jednog čoveka može biti drugom čoveku informacija*. U skladu s tom izjavom i Rumizen[41] upozorava na zamku svrstavanja znanja u kategorije podatak, informacija ili znanje. Odavde se može zaključiti da kontekst odvaja navedene kategorije, te nešto što je za jednu osobu znanje za drugu može biti samo informacija i obrnuto.

2.1.2 Kategorizacija znanja

Znanje u kompaniji je više dimenzionalno i dinamično, a može biti u eksplicitnoj i prećutnoj (implicitnoj) formi. [42] Isto tako, može se izvršiti kategorizacija znanja na način u kome jedan ekstrem predstavlja tacitno, a drugi eksplicitno znanje [43], pri čemu sama granica između njih nije jasno povučena. [44] Znanje ima materijalni i nematerijalni oblik koje se razlikuju prema:

- mogućnosti i težini iskazivanja, kodifikovanja i prenošenja,
- načinima za sticanje, akumuliranje i prenošenje.

Ova dva oblika znanja u praksi kompanija, najvećim delom, su povezana, odnosno u međusobnoj su interakciji iz koje se stvara i novo znanje. Ključno za svaku kompaniju je da privuče kompetentne izvršioce, sa kvalitetnim, vrednim i jedinstvenim individualnim, implicitnim znanje. Pored toga, važno je da se izvršioci stimulišu da to znanje prenose, šire kroz kompaniju (koristeći ga u izvršavanju zadataka i obavljanju radnih procesa), dakle, da se mobiliše implicitno znanje radi njegove što brže i kvalitetnije konverzije u eksplicitno (kolektivno, organizaciono) znanje.

Pravilna podela znanja sa aspekta strategija menadžmenta znanja je ona koja posebno izdvaja implicitno (engl. *tacit*) a posebno eksplicitno (engl. explicit) znanje. Suština eksplicitnog znanje je u njegovom izražavanju kroz formalni jezik i razmenjivanju između individua, dok je implicitno znanje lično znanje koje se ogleda u individualnom iskustvu i uključuje apstraktne faktore kao što su lična uverenja, perspektive i vrednosti. [45]

2.1.2.1 Eksplicitno i prećutno znanje

Eksplicitno znanje (materijalni oblik) sadržano je u planovima, projektima, patentima, proizvodima/uslugama i bazama podataka. Ono se može izraziti formalnim, sistematičkim jezikom i razumeti (preneti) u obliku podatka, specifikacije i uputstava. Zato se i kaže da je ono formalno i dokumentovano. Kao takvo, najpre, može biti opisano u dokumentima, zatim procesuirano (obrađeno i transformisano), i preneto kroz poslovni sistem odgovarajućim informacionim sistemom i sačuvano pomoću savremene informacione i druge tehnologije. Eksplicitno znanje je, ponekad, prilikom upotrebe „nevidljivo" i kompleksno, jer predstavlja rezultat iskustva, višegodišnje prakse, a može biti pribavljeno eksterno, ali i kreirano interno, a onda povezano, pa predstavljati element organizacije kao sistema.

Informaciona tehnologija čini eksplicitno znanje još eksplicitnijim i omogućava da se ono u sistemu brzo širi i da se na taj način bolje iskorišćava. Kompanija koja ima brz prenos i širenje eksplicitnog znanja kroz organizaciju stvara konkurentsku prednost u

odnosu na rivale koji vrše sporije transformaciju znanja (informacije) između svojih organizacionih (poslovnih) jedinica, kao i do pojedinaca na različitim radnim mestima. Preslikavanjem se eksplicitno znanje može brzo preuzeti i preneti do konkurenata, pa je zbog toga posebno važna njegova zaštita u nekoj formi intelektualne svojine. Njegova osnovna karakteristika je lako prenošenje i prikuplja se kroz slušanje ili čitanje, dok je tacitno znanje komplikovano za razumevanje i prenošenje. U tabeli broj 1 prikazana je razlika između karakteristika tacitnog i eksplicitnog znanja.

Tabela 1. *Uporedni prikaz karakteristika tacitnog i eksplicitnog znanja*
Izvor: [46]

Tacitno znanje	Eksplicitno znanje
Znanje iz iskustva	Racionalno znanje
Simultano znanje (ovde i sada)	Sekvencionalno znanje (tamo i tada)
Poznavanje prakse	Poznavanje teorije

Prećutno, implicitno ili skriveno znanje (nematerijalni oblik) podrazumeva znanje zaposlenih, njihove ideje, vizije, veštine, iskustva, sposobnosti, kulturu i dr. Ovakvo znanje je previše lično, tako da ga je teško formalizovati, pa se zato ističe da je ono nedokumentovano i neformalno. Za razliku od eksplicitnog znanja, prećutno – implicitno znanje čine i stručne kompetencije, prosuđivanje i intuicija zaposlenih. Duboko je ukorenjenjo u delovanje, praksu i razmišljanje pojedinca, kao i posvećenost specifičnom problemu/poslu.

Menadžment prećutnim znanjem (posebno, veštinama i intuicijama) veoma je kompleksan zato što ga je teško izraziti u eksplicitnoj formi. Isto tako, nekada pojedinac nije ni svestan znanja koje ima, pa onda nema ni njegovog prenosa drugima. Prećutno znanje koje je pojedinac prethodno stekao i upotpunio radeći u kompaniji, njegovim odlaskom „napušta" i samu kompaniju. Taj gubitak za jednu kompaniju može biti sa velikim posledicama ukoliko se radi o zaposlenima na visokom nivou odlučivanja. Prećutno znanje koje pojedinac „ponese" iz kompanije „štiti" se u formi *know-how*/poslovne tajne ili, eventualno, ugovorom zaposlenog sa poslodavcem kojim se zabranjuje rad u konkurentskoj firmi, osnivanjem biznisa u istoj delatnosti i dr. Po Jeleni Đorđević Boljanović značaj prećutnog znanja je što se sve inovacije i kreativni procesi baziraju na toj vrsti znanja. [47]

Polazeći od razlika eksplicitnog i implicitnog, znanje se može kategorizovati i na sledeći način: [47]

- Iskustveno znanje – u suštini prećutno (implicitno) znanje – stvarano je i razmenjivano vremenom kao iskustvo (ovde se ubrajaju veštine *know-how* zaposlenih koje se stiču postepeno kroz rad).
- Konceptualno znanje – sastoji se od eksplicitnog znanja koje je artikulisano pomoću slika, simbola, jezika (koncepti proizvoda, dizajni i marke proizvoda).
- Rutinsko znanje – implicitno znanje sadržano u akcijama i praksi (*know-how* u svakodnevnim radnim aktivnostima – operacijama, organizacionim rutinama i kulturi).
- Sistemsko znanje – eksplicitno znanje, sistematizovano i inkorporirano u strategijama, dokumentima, specifikacijama, uputstvima, bazama podataka, patentima i licencama.

Pored dve osnovne kategorije znanja – tacitnog i eksplicitnog, u literaturi se mogu naći i druge vrste znanja, gde svaka od njih ima svoju svrhu i specifične osobine koje su

predstavljene u tabeli 2.

Tabela 2. *Prošireni popis kategorije znanja sa primerima*
Izvor: [38]

Vrsta znanja	Definicija	Primer
Tacitno	Znanje koje je ukorenjeno u akcijama i iskustvu, a povezano je sa specifičnim kontekstom.	Najbolji način odnošenja sa određenim kupcem.
Kognitivno tacitno	Mentalni modeli.	Uverenja pojedinaca o odnosima uzrok–posledica
Tehničko tacitno	Znanje kako se nešto radi (eng. *know-how*) primenjivo na specifičan posao.	Veština izvođenja hirurške operacije.
Eksplicitno	Jasno izraženo, generalizovano znanje.	Znanje o najvažnijim kupcima u regiji.
Individualno	Kreiraju i koriste pojedinci.	Spoznaje iz završenog projekta.
Socijalno	Kreiraju i koriste grupe.	Norme za komunikaciju unutar grupe.
Deklarativno	Poznavanje činjenica o nekoj tematici (eng. *know-about*).	Koji lek je odgovarajući za određenu bolest.
Proceduralno	Znanje kako se nešto radi (eng. *know-how*).	Kako se primenjuje određeni lek.
Kauzalno	Razumevanje uzroka (eng. *know-why*).	Razumevanje kako određeni lek deluje.
Vremenski uslovljeno	Razumevanje veza sa drugim temama ili pitanjima (eng. *know-with*).	Razumevanje kakve interakcije može imati lek sa nekim drugim lekom.
Pragmatično	Znanje korisno za organizaciju.	Najbolja praksa, iskustva sa projekata, izveštaji o tržištu.

Pored opsežnog popisa kategorija znanja navedenih u tabeli 2, Tsai i Lee tvrde da se može definisati i znanje koje proizlazi iz duboke motivisanosti kreativnosti pojedinca kome je važno da razume uzroke (engl. *care-why*)[48] kao i znanje koje je direktna posledica veštine povezivanja, a proizilazi iz poznavanja širokog kruga osoba kojima se neko može obratiti (tzv. *know-who*). Imajući u vidu činjenicu da je znanje predmet konstantnih preispitivanja i proučavanja, očekuje se u budućnosti proširivanje popisa specifičnih kategorija znanja.

Kada se govori o kategorijama znanja zavisno od njegovog doprinosa uspešnosti kompanije, ono se može sagledati i kroz model koji daju Hicks, Dattero i Galup [49], a uključuje pet stepeni u hijerarhiji znanja: *individualno znanje*, koje se nalazi u umovima pojedinaca; *činjenice*, koje se čuvaju u pisanom obliku, bazama podataka i skladištima podataka; *uticaji*, činjenice odnosno podatke pripremljene za prezentovanje, a koji dolaze do izražaja u sistemima podrške donošenju odluka, sistemima učenja, žutim stranicama i izveštajima; *rešenja*, odnosno jasna uputstva kako se izvodi određeni zadatak, koja se prezentuju primerima kroz prenošenje najbolje prakse; *inovacije* koje podrazumevaju korišćenje resursa koji se temelje na znanju (engl. *knowledge based resources*).[49]

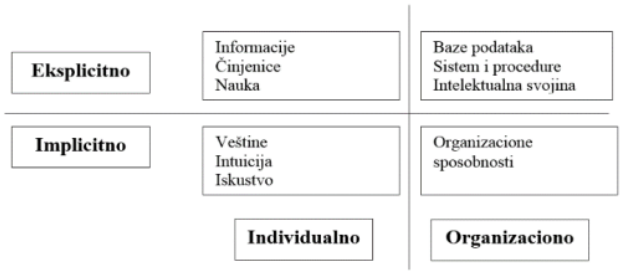
2.1.2.2 Individualno i organizaciono (kolektivno) znanje

Znanje koje je smešteno u glavama zaposlenih za razliku od nematerijalnog znanja neprikosnoveno je vlasništvo pojedinaca, a znanje u materijalnom obliku može biti svojina kompanije. Individualno znanje je potrebno za rešavanje specifičnih zadataka i problema. Pojedinac sa svojim znanjem je autonoman u korišćenju svog individualnog znanja, kao i prenosu tog znanja drugima. Kompanija raspolaže prećutnim znanjem samo dok su njegovi vlasnici tj. zaposleni – fizički prisutni u kompaniji. Upravo zbog toga, cilj menadžemnta svake kompanije je da izvrši kodifikaciju, tj. konvertuje prećutno znanje pojednica u eksplicitno, organizaciono (kolektivno) znanje.

Organizaciono (kolektivno) znanje zavisi od sposobnosti konverzije individualnog znanja u kolektivno, ali i od konverzije jednog organizacionog znanja, u novo, veće,

sadržajnije, kvalitetnije, organizaciono znanje. Za konverziju ovakvog tipa veliki značaj ima način na koji se znanje širi, razmenjuje, tj. deli između članova u kompaniji. Konverzijom se individualno znanje ugrađuje u procese, proizvode, usluge, procedure, rutine, *know-how*, organizaciona pravila, norme, vrednosti koje određuju načine rešavanja praktičnih problema. Kolektivno znanje, većim delom, rezultat je interakcije znanja pojedinaca, pa se može reći da je skup individualnih znanja.

Individualno i organizaciono znanje može biti eksplicitno i implicitno (slika 3). Vukšić u svojim istraživanjima tvrdi da se kolektivno znanje vidi kao znanje u „čvrstoj formi", tj. kao određeni fond znanja kompanije koje je u različitim formama (dokumentima, bazama podataka, metodama rada i menadžmenta, tehnologijama, projektima, procedurama, praksama, iskustvima, proizvodima i uslugama, ekspertizama, sposobnostima, kompetencijama, ključnim kompetencijama). Međutim, kolektivno znanje može biti i u „fluidnom" obliku, može da se kreće kroz kompaniju kao rezultat komunikacije i interakcije članova više organizacionih delova kompanije. Organizaciono ili kolektivno znanje određuje sposobnost da se obavlja neka privređivačka aktivnost.[50]



Slika 3. *Eksplicitno i implicitno, individualno i organizaciono znanje*
Izvor: [46]

Prema tvrdnjama Nonake i Takeučija znanje se pretvara kroz (slika 4): socijalizaciju, eksternalizaciju, kombinaciju i internalizaciju. [46] Ono se stvara interakcijom eksplicitnog i implicitnog znanja i transformacijom (konverzijom) jednog tipa znanja u drugi. Ovo je *SECI* spiralni proces, zbog „toka znanja", tj. redosleda kretanja znanja iz faze u fazu: od socijalizacije (S – engl. *Socialization*), ka eksternalizaciji (E – engl. *Externalization*), od eksternalizacije ka kombinaciji (C – engl. *Combination*), od kombinacije ka internacionalizaciji (I – engl. *Internalization*), od internacionalizacije ka socijalizaciji, i tako redom u krug.



Slika 4. *Eksplicitno SECI proces konverzije znanja*
Izvor: [46]

Socijalizacija predstavlja prenošenje implicitnog znanja od jedne do druge osobe

balnim učenjem, posmatranjem, ugledanjem – imitacijom, pokazivanjem radnji). Pojedinac prenosi znanje drugom članu u kolektivu ili ga zaposleni dobija (prima) od lica van kompanije (poslovnog partnera, konsultanta, eksperta, inspektora i sl.). Korisnik tog znanja na taj način stiče znanje u implicitnoj formi. Socijalizacija se ostvaruje na više načina: formalnom komunikacijom (usmeno, u pisanoj formi, elektronskom obliku i sl.), neformalnom komunikacijom, diskusijom tokom posla, postavljanjem pitanja, posmatranjem kako se izvršavaju poslovi, učenjem i obukom uz rad, neformalnim sastancima van radnog vremena, komunikacijom i interakcijom sa ljudima van kompanije i dr. Prećutno znanje je ponekad teško „podeliti" u jednoj kompaniji iz više razloga, kao što su: loši međuljudski odnosi, nespremnost da se nauče zaposleni, nespremnost da se informacije razmenjuju, da se prenese iskustvo ili postojeća individualna praksa. Zbog svega ovoga nužna je eksternalizacija. [46]

Eksternalizacija predstavlja konverziju implicitnog u eksplicitno znanje. Ta konverzija uključuje da znanje koje poseduje jedna osoba a koja ga istovremeno i oblikuje, prenosi drugoj osobi, koja ga, pak, naknadno pretvara u eksplicitnu formu. U eksplicitnoj formi, ono može da se razmenjuje sa drugim članovima kompanije i postaje osnova za stvaranje novog znanja i uvećanje postojećeg znanja. Procesom eksternalizacije implicitno znanje pojedinca postaje, vidljivo, obelodanjeno, dokumentovano i zabeleženo. [46][47]

Kombinacija definiše transformaciju eksplicitnog znanja u složeniju formu. Predstavlja proces povezivanja koncepata (eksplicitnih) u sistem znanja u cilju stvaranja novog znanja. Tako, na primer, dokumenti ili informacije se razmenjuju i uvećavaju „memoriju organizacije" (organizacionu bazu podataka). Kao takvi, sada, mogu da se koriste za razvoj sopstvenog, prećutnog znanja što se naziva procesom internalizacije.

Internalizacija je proces pretvaranja eksplicitnog znanja u implicitno znanje. Eksplicitno znanje koje je u kompaniji stvoreno i šireno kroz nju, može se internalizacijom konvertovati u implicitno znanje pojedinaca. Povezana je sa učenjem kroz rad. Eksplicitno znanje se može aktualizovati kroz akciju i praksu primenom koncepta proizvoda ili procedura proizvodnje. Tako se na primer, programima obuke pomaže zaposlenima da razumeju funkcionisanje kompanije i svoje uloge (zadatka) u njoj. [42][47]

Efektivnost znanja ogleda se u efektima koje donosi pri obavljanju svakodnevnih poslovnih aktivnosti u odnosu na planirane efekte pri njihovom izvršavanju. Ona je, determinisana stepenom uspešnosti ostvarivanja ciljeva koji se realizuju uz pomoć određenog znanja. Zbog toga se i kaže da je efektivno ono znanje koje omogućava poboljšanje internih procesa, kvalitetnije odlučivanje i rešavanje problema.

Efikasna upotreba znanja ogleda se u njegovom brižljivom kodifikovanju (pretvaranju znanja u dokumenta, slike, reči), kao i skladištenju postojećeg znanja u elektronskim bazama podataka („memoriju organizacije"), kako bi se ponovo koristilo i na taj način smanjili troškovi poslovanja. Ostvaruje se kada se znanje koje je potrebno lako obezbeđuje i koristi od strane pojedinca ili kompanije i ukoliko se tokom vremena efekti od njegove upotrebe uvećavaju u odnosu na ulaganje koje je izvršeno za njegovo generisanje. Efikasnost znanja se postiže i ako je znanje tako strukturirano da se relativno jednostavno uvećava, obnavlja i pretvara u neke druge oblike.

Menadžment znanja mora biti prilagođen tako da znanje koje se koristi odgovara okruženju i željenim funkcijama kompanije. Takođe, menadžment znanja treba da bude dobro povezan i usaglašen sa drugim aktivnostima u kompaniji: istraživačko-razvojnim, proizvodnim, marketinškim i investicionim. Aktivnosti menadžmenta znanja treba da se izvršavaju tako da omoguće održavanje postojećih resursa znanja kao visokog razvojnog prioriteta.

Kompanijama je mnogo veći problem kako sprovoditi menadžment implicitnim nego eksplicitnim znanjem. Obzirom da implicitno znanje nigde nije zapisano ono je u suštini imanentan deo svake ličnosti koja ga poseduje. Najčešće se prenosi govorom, međusobnim diskutovanjem, otvorenim sugestijama i za njegov transfer je neophodna želja i volja onoga ko ga poseduje da ga prenese drugome. U ovoj činjenici se ogleda problem menadžmenta implicitnim znanjem u slučajevima fluktuacije radnika ili njihovog odlaska u penziju. Prelazak radnika u neku drugu kompaniju koja time na poklon dobija implicitno znanje novopristiglog radnika bez ikakvih ulaganja veći problem za kompanije u odnosu na odlazak radnika u penziju. Jedno rešenje ovog problema leži u kodifikaciji implicitnog znanja, što predstavlja negov prelazak u eksplicitni oblik. Implicitno znanje upotrebom odgovarajućih simbola prelazi u eksplicitno znanje.

2.2 Niz međusobnih interakcija u kreiranju inovacije znanja

Da bi proces menadžmenta znanja u kompaniji bio uspešan, preduslov je primena koncepta tzv. lanca znanja (engl. *knowledge chain*) pomoću koga je moguće prikazati niz međusobnih interakcija važnih u kreiranju organizacionog ciklusa inovacije znanja. Ovaj izraz prvi su uveli autori Koulopoulos, Toms i Spinello. [51] Kako bi kompanija održala konkurentsku prednost postoje četiri važna elementa u lancu znanja od kojih zavisi jedinstvenost, specifičnost i dugotrajno održavanje. [52] Elementi koji čine suštinu korisnosti menadžmenta znanja su: [47][53]

- interna svest kompanije (engl. *internalawarness*),
- interna odgovornost (engl. *internal responsiveness*),
- eksterna svest (engl. *external awarness*) i
- eksterna odgovornost (engl. *external responsiveness*).

Interna svest kompanije predstavlja sposobnost brze procene njenih ključnih kompetencija i njenih ukupnih veština. Problem se javlja kod onih kompanija čija se delatnost odvija prema određenim definisanim pravilima u okviru funkcione strukture. Ovakve kompanije svoju ključnu kompetenciju vezuju samo uz postojeće proizvode ili usluge, ne sagledavajući pri tome i važnost poznavanja svojih znanja, veština i sposobnosti bitnih za dalji razvoj. [53]

Interna odgovornost se ogleda sposobnošću kompanije da upotrebom sopstvenih znanja i ključnih kompetencija izvrši njihovo što brže ugrađivanje u novi proizvod ili uslugu i ponudi kupcima na tržištu. [53]

Eksterna svest kompanije predstavlja njenu sposobnost da što tačnije proceni položaj svojih proizvoda ili usluga na tržištu, pravovremeno uoči tržišne trendove, želje i navike kupaca, ali i da prepozna opasnosti koje joj prete od novih konkurentskih aktivnosti, kao i da vodi brigu o institucionalnim ograničenjima, novim propisima itd. [54]

Eksterna odgovornost, može se okarakterisati kao sposobnost kompanije da se prilagođava zahtevima tržišta brže i uspešnije od njenih konkurenata. Predstavlja suštinu konkurentske prednosti i pitanje opstanka na tržištu.

U tabeli 3, dat je prikaz elemenata lanca znanja sa aktivnostima kroz primer dve vrste kompanija, u onima koje prihvataju koncept menadžmenta znanja, tzv. organizacijama koje stalno „uče" i onima sa tradicionalnim pristupom – tradicionalna organizacija.

Jedan od strateških prioriteta poslovanja, prepoznat i prihvaćen od najviših nivoa menadžmenta u kompaniji mora biti i potreba za novim znanjem. U tom pogledu, potreban preduslov je izgradnja organizacione kulture i razvoj mehanizama za deljenje znanja. Kada se stvore neophodni preduslovi za razmenu znanja, potrebno je analizirati i definisati prostor između raspoloživog i potrebnog znanja, a nakon toga razviti mehanizme i metrike procene i reprodukcije znanja. Krajnji cilj treba da bude postizanje sinergijskih efekata primenom kombinacije procesuiranja podataka i informacija uz upotrebu informacionih tehnologija zajedno sa kreativnim i inovativnim sposobnostima svojih zaposlenih.[53]

Tabela 3. *Elementi lanca znanja sa aktivnostima*
Izvor: [52]

	Unutrašnja	**Spoljašnja**
SVESNOST	***Organizacija koja stalno „uči"***	
	kolektivna svest o snazi i slabostima unutra i kroz funkcionalne strukture, iskustva se otvoreno prenose, fokus je na kompetencijama i talentima, a ne na proizvodima	unapred razmišlja o mogućim konkurencijama, kontinuirano otklanja prepreke i istražuje inovativne pristupe za osvajanje novih klijenata
	Tradicionalna organizacija	
	slaba unutrašnja svesnost, rukovođenje svesno hijerarhijski prema određenoj funkcionalnoj strukturi, statična politika i procedure, znanje se deli, fokus je na postojećoj proizvodnji	oslanjanje na postojeće robne marke, ne pridaje se dovoljno pažnja na istraživanja novih mogućnosti za zadržavanje postojećih i osvajanje novih kupaca, vrlo mali napori u aktivnostima predviđanja kretanja tržišta
	Unutrašnja	**Spoljašnja**
REAKTIVNOST	***Organizacija koja stalno „uči"***	
	sposobna je odmah da koristi sve svoje veštine na osnovu sprovedene interne procene svojih resursa i procene novih zahteva i mogućnosti na tržištu	fokus usmerava na nove proizvode/ usluge kupcu, koje su rezltat njenog znanja i dodatne vrednosti proizvodu iako ih tržište još nije artikulisalo i što je povraćaj uloženih sredstava neizvestan
	Tradicionalna organizacija	
	nove idele „guše" se zbog oslanjanja na unapred utvrđene procedure i strogi hijerarhijski stil donošenja odluke u okviru jedne organizacione strukture	dugi periodi između inovacionih ciklusa, nerazvijeni distribucioni kanali sa standadizovanim proizvodima

Ovde možemo zaključiti da kompanije kako bi zadržale mesto na tržištu i ostvarile određeni iskorak u tehnološkom ili nekom drugom smislu, ili pak postale vodeće u svojoj oblasti poslovanja, moraju staviti poseban akcenat na izgradnji elemenata vlastite infrastrukture menadžmenta znanja. Da bi kompanija bila uspešna, ona neprekidno mora usvajati nova znanja, dok menadžment kompanije to usvajanje znanja mora postaviti kao jedan od važnih prioriteta u poslovanju kompanije. Krajnji cilj svake uspešne kompanije je ostvarenje zajedničkog efekta kombinacijom procesuiranja podataka i informacija uz primenu informacionih tehnologija, uz uključivanje inovativne i kreativne sposobnosti sopstvenih kadrova sa krajnjim ciljem donošenja kvalitetnijih poslovnih odluka. Važnost lanca znanja ogleda se u tome što svojim interakcijama može dovesti do serije inovacija u kompaniji. Što je propustljivost između veza u kompaniji veća, veća je i brzina inovacija. [57]

2.3 Strategije menadžmenta znanja

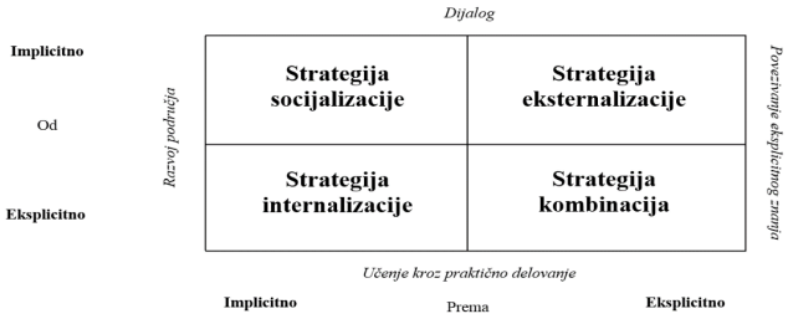
Strategije menadžmenta znanja primenjuju se u funkciji ostvarivanja konkurentske prednosti kompanije. Povezana je sa poslovnom strategijom kompanije i podržava je. Njihov odnos je komplementaran i treba da rezultuje u proizvodima i uslugama koji su bazirani na znanju (engl. *knowledge based products*) i koji mogu sebi da obezbede mesto na tržištu.

Strategije menadžmenta znanja se dele u dve osnovne kategorije. U prvu spadaju generičke strategije menadžmenta znanja koje su vezane za prelazak znanja iz jednog oblika u drugi, dok drugu čine opšte strategije menadžmenta znanja koje su u vezi sa načinima ostvarivanja konkurentske prednosti upotrebom znanja.

2.3.1 Generičke strategije menadžmenta znanja

Kategorizacija znanja na eksplicitno i implicitno predstavlja osnovu za definisanje generičkih strategija menadžmenta znanja. Takođe, ovo je najznačajnija podela znanja i osnova je za ostale kategorizacije.

Eksplicitno znanje se izražava na formalnom jeziku i razmenjuje između individua, dok je implicitno znanje oličeno u individualnom iskustvu i uključuje neopipljive faktore kao što su lična uverenja, perspektive i vrednosti. [45] Na slici 5 uočava se da postoje četiri generičke strategije menadžmenta znanja. Mogu samostalno da egzistriraju, ali se one u praksi kombinuju, jer se samo u tom slučajum može obezbediti potpun menadžment znanja.



Slika 5. *Četiri generičke strategije menadžmenta znanja*
Izvor: [46]

Strategija socijalizacije – definiše prenos implicitnog znanja sa jednog subjekta na drugi. U suštini predstavlja imitiranje metoda i procesa rada, kao i ponašanja u izvršavanju zadataka i vezano je za rutinske operacije zaposlenih. U svrhu prenošenja ovog znanja, neophodno je da subjekat koji ga usvaja bude u fizičkom konktaktu sa subjektom koji ga emituje, mada postoje mogućnosti da se transfer ovakvog znanja vrši telekomunikacionim putem, gde se može javiti problem eventualnih nesporazuma i štete nastale po osnovu nerazumevanja.

Strategija eksternalizacije – predstavlja proces prelaska implicitnog u eksplicitno znanje. Zasniva se na kodifikaciji implicitnog znanja na trajni medijum koji poseduje standardizovan fizički oblik. Prelaskom implicitnog u eksplicitno znanje kompanija štiti sebe od gubitka akumuliranog implicitnog znanja iz ranijeg perioda i čuva ga od zaborava. Na taj način skraćuje vreme potrebno da se praksa iz prošlosti ponovi u budućnosti i smanjuje troškove potrebne da se ponovo postigne potrebni nivo eksplicitnog znanja

neophodnog za izvršavanje određene operacije ili zadatka.

Strategija kombinacije – definiše nadograđivanje postojećeg eksplicitnog znanja. Znanje koje je zapisano na nekom medijumu može da bude predmet interesovanja i da u kombinaciji sa novom idejom rezultuje u kreiranju novog znanja koje dalje može biti predmet neke nove nadogradnje ili transfera u implicitno znanje.

Strategija internalizacije – predstavlja postupak prelaska eksplicitnog u implicitno znanje. U suštini je primena znanja u praktične svrhe. Praktičnom proverom se verifikuju teorijski razrađene postavke problema se.

2.3.2 Opšte strategije menadžmenta znanja

Konsultantska kuća *McKinsey & Company*, shodno Day i Wendler [58] identifikovali su pet strategija menadžmenta znanja koje koriste velike korporacije. Ovakvoj kategorizaciji može se zameriti to što favorizuje velike kompanije.

Strategija razvoja i transfera najbolje prakse – fokusirana je na identifikaciju najboljih praksi u okviru kompanije i na njihovo širenje preko mreže lokacija. Ideja o primeni najboljih praksi nije nova, ali tek u okviru koncepta menadžmenta znanja dobija svoje teorijsko utemeljenje. Strategija može da se koristi komplementarno sa konceptom *benchmarking*. [58]

Strategija oblikovanja korporativne strategije na osnovu znanja – bazirana je na postojećem znanju kompanije kroz preispitivanje uslova okruženja i strategijskih opcija. Ovakvom strategijom formulišu se potrebe za znanjem tako da se u skladu sa strategijskim prioritetima vrši konstantno nadogradnja znanja kompanije. Proces je ireverzibilan što zapravo znači da novostečeno znanje može da kreira nove mogućnosti koje zahtevaju reformulisanje korporativne strategije. [58]

Strategija stvaranja i komercijalizovanja inovacija – fokusirana je na jačanje konkurentske pozicije kroz uvećanje broja tehnoloških inovacija. Cilj primene ove strategije je skraćivanje vremena potrebnog za razvoj novog proizvoda i njegovu komercijalizaciju.[58]

Strategija definisanja standarda oslobađanjem sopstvenog znanja – ima široku primenu u softverskoj industriji i izrazito je uspešna u primeni menadžmenta znanja. Primenom ove strategije, kompanije povećavaju svoje tržišno učešće, poboljšavaju ugled, dobijaju poverenje korisnika i na kraju, što je možda i najvažnije, dobijaju povratnu informaciju od korisnika o tome na koji način je moguće izvršiti poboljšanje samog softvera. Povratne informacije korisnika prelaze u korisno znanje koje doprinosi povećanju vrednosti proizvoda kompanija

2.3.3 Elementi strategije menadžmenta znanja

Svaka strategija menadžmenta znanja sadrži različite elemente koji su manje ili više važni za svaku od njih. Stalni činioci koji se pojavljuju u svakoj strategiji su: ljudi, tehnologija i procesi. U nastavku rada biće predstavljen skup uobičajenih elemenata strategije menadžmenta znanja.

Menadžment znanja sadrži dva važna elementa koji se međusobno dopunjavaju: ljudi i informacione tehnologije, bez kojih ne bi postojala strategija menadžmenta znanja. Ljudi i informacione tehnologije su danas u potpunosti nerazdvojni i međusobno su zavisni. Između tih elemenata postoji niz elemenata vezanih za znanje i njegovu upotrebu. [59]

Ljudi će uvek predstavljati ključan element menadžmenta znanja bez obzira na

činjenicu da danas tehnologije preuzimaju uloge ljudi i poslove realizuju bolje i brže. Čuvanje znanja ne znači da bez uključivanja čoveka taj sistem neće biti produktivan. Sakupljanje znanja i njegovo smeštanje na jedno mesto ne obezbeđuje njegov dalji razvoj i primenu bez učešća ljudi. S druge strane, ljudi u svim procesima menadžmenta znanja mogu pokazati svoje najslabije tačke. Ipak, čovek poseduje iskustva, vrednosti i svesnost konteksta kada se porede sa mašinama i tehnologijom.

Razvoj kompanija zavisi od veština i znanja zaposlenih, njihovih talenata i nivoa angažovanja. To je važno pitanje koje se odnosi na ljudski faktor. Vlasnik svake kompanije treba sagledati svoje zaposlene kao vredne resurse, sposobne ne samo da izvršavaju postavljene zadatke, već i kao kapital u koji se isplati ulagati. Pored toga i ambijent i kultura u svakoj kompaniji je veoma bitna. Poznato je da je otvorenost i prihvatanje utičnu na bolji razvoj kompanije u odnosu na individualističke kulture i takmičenja [60].

Informaciona tehnologija sadrži potpune modele, akcije i mere vezane za obradu informacija. Ona predstavlja kombinaciju informacione tehnologije i telekomunikacija, hardvera, softvera i drugih tehnologija vezanih za prenos, čuvanje, obezbeđivanje i prezentovanje znanja. Kao takva, omogućava alate za dobijanje informacija, njihov izbor, analizu, prikupljanje i deljenje sa drugima što čini ključne aspekte menadžmenta znanja. Zahvaljujući ovim tehnologijama, kompanija ostvaruje: brzu i produktivnu komunikaciju, produktivno deljenje znanja i alate za kreiranje znanja. Informacioni sistem koji podržava menadžment znanja u kompanijama kreiran je kako bi pomogao u dobijanju informacija iz različitih kanala, kodifikaciji, pripremi novog znanja i njegovo deljenje.

Informaciona tehnologija omogućava brojne alate koji su podložni izmenama. Bez tih izmena menadžment znanja ne bi bio moguć. Izmene su rezultat sledećih činilaca: potrebe za interpretacijom informacija, uočavanjem mogućih grešaka i njihovom korekcijom, razvojem hard disk memorije (engl. *hard memory*), baza podataka, kao i potrebe za dobijanjem informacija i njihovim praćenjem.

Procesi predstavljaju elemente koji uključuju znanje. Različiti autori definišu različite procese, ali se uglavnom svodi na: detekciju znanja, kreiranje znanja, deljenje znanja, implementaciju i korišćenje znanja, čuvanje znanja i njegovo ažuriranje.

Detekcija znanja predstavlja utvrđivanje statusa, mesta i izvora znanja, postojećih aktivnosti i iskustava, uloge unutar kompanije, strukturna znanja i iskorišćavanja, koristi za kompaniju i prepreke za dalji napredak. Veoma je važno poznavati cilj kompanije, dok lociramo znanje. Može se odrediti lokacija internog i eksternog znanja. Kada govorimo o internom znanju, njegova lokacija može imati nekoliko aspekata, kao što su:

- određivanje lica koja poseduju znanje,
- odabir informacija koje pripadaju resursima znanja,
- otkrivanje prećutnog znanja i njegovo deljenje,
- svesnost naših ličnih grešaka i praznina,
- traženje skrivenih resursa kompanije,
- baza za izmene u primeni znanja.

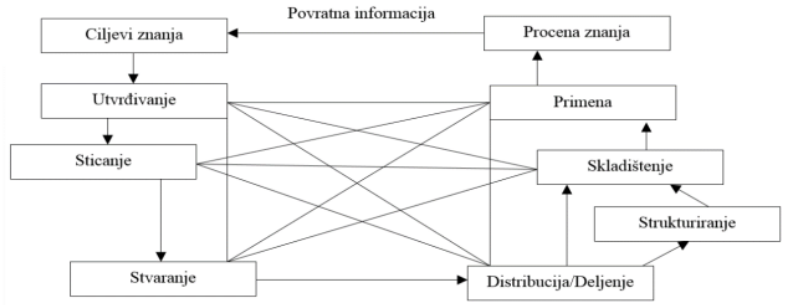
Eksterna lokalizacija znanja odnosi se na upoznavanje sa okruženjem kompanije i pravilima koja ga određuju. Korisni alati koji mogu pomoći u postizanju tog cilja uključuju primenu mapa znanja: mentalnih mapa, mapa resursa znanja, dijagram riblje kosti (engl. *fishbone diagram*) ali i sve druge alate koji mogu pomoći u određivanju lokacije znanja (npr. upitnici i komunikacioni alati).

Pre samog kreiranja znanja, kompanija treba da da odgovore na pitanja o viziji znanja. Istraživači definišu dve vrste znanja koja se javljaju u kompaniji, a to su eksplicitno i tacitno znanje. Eksplicitno znanje može biti izvor raznih ideja i inovacija tako da ga je jednostavno deliti putem uobičajenih oblika komunikacionih i informacionih tehnologija. Tacitno znanje je teško jasno definisati, jer se uglavnom prenosi usmenim putem. Lični kontakti i timski rad predstavljaju najbolji način za razvoj i deljenje takve vrste znanja. Kreiranje znanja sastoji se od različitih faza, a to su:

- sticanje znanja (prikupljanje znanja iz internih i eksternih kanala) i
- razvoj znanja (primena analogija i metafora, popis nedostataka i razgovor o njima, kreativno razmišljanje (engl. *brainstorming*), grupni rad – postavljanje prioriteta i dr.).

Deljenje znanja podrazumeva deljenje eksplicitnog i tacitnog znanja u okviru kompanije. Deljenje eksplicitnog znanja podrazumeva deljenje prikupljenih i obrađenih informacija koje dopiru do ljudi koje interesuju rezultati analiza. Deljenje tacitnog znanja predstavlja prenos znanja sa jednog zaposlenog na drugog, primenom ličnog kontakta, kao i alate informacionih tehnologija.

Implementacija i korišćenje znanja koristi se u bilo koje vreme. Ovo potencira važnost da se znanje može identifikovati i koristiti u pravo vreme i na pravom mestu. Implementacija znanja uglavnom zavisi od ličnih veština zaposlenih. Prilikom implementacije znanja, potrebno je dati akcenat na: razvoju veština drugih, izgradnji produktivnih timova, strateškom razmišljanju i delovanju, iskorišćavanju i umnožavanju znanja i poboljšavanju produktivnosti rezultata.



Slika 6. *Temeljne komponente menadžmenta znanja*
Izvor: [61]

Čuvanje znanja i njegovo ažuriranje sastoji se od: izbora znanja; čuvanja znanja, ažuriranja znanja i procene znanja u smislu određivanja koliko je to znanje zaista i korisno.

2.3.4 Izrada strategije menadžmenta znanja

Strategija menadžmenta znanja je veoma bitna za svaku kompaniju, jer unapređuje njenu konkurentnost i uspešnost. Pravilno razvijena strategija može doprineti u ostvarivanju ciljeva svake kompanije. Pored toga, ona donosi usklađenost sa načinom poslovanja kompanije, poboljšava produktivnost i zadovoljstvo zaposlenih i smanjuje troškove. U ovom delu rada, biće predstavljeno na koje se načine strategija menadžmenta znanja može razviti i koji su potrebni elementi za to.

Razvoj strategije menadžmenta znanja može se sprovesti na nekoliko načina. Ne možemo tvrditi da će svaka strategija odgovarati svakoj kompaniji. Svaka strategija menadžmenta znanja treba da definiše način unutar kompanije koji će biti upotrebljen za

menadžment znanja; na koji način će se kompanija menjati kako bi obezbedila funkcionisanje strategije; koje će se aktivnosti vršiti; ko će biti odgovoran za sve aktivnosti i kako će se čitav posao izvršiti; koja će se tehnologija koristiti za podršku i deljenje znanja. Zahvaljujući informacionoj tehnologiji, menadžment znanja je znatno olakšan. [59]

Tabela 4. *Strategija menadžmenta znanja*
Izvor: [59]

Gde se trenutno nalazimo?	Procena postojeće situacije. Kako postojeća praksa upravljanja znanjem (ili njen nedostatak) utiče na sposobnost organizacije da postigne svoje ciljeve? Kako utiče na produktivnost pojedinaca i timova? Kakve vrste znanja stvaramo, prikupljamo i čuvamo? Kakve smo rezultate ostvarili? Na koji način kultura i sistemi naše organizacije odgovaraju ili ometaju upravljanje znanjem?
Gde želimo da budemo?	Opis onoga što upravljanje znanjem može učiniti za organizaciju. Kako će pomoći organizaciji i njenim zaposlenima da ostvare svoje ciljeve? Kako bi izgledala dobra praksa upravljanja znanjem za ovu određenu organizaciju? Na koji će način strategija upravljanja znanjem izmeniti našu organizaciju u narednih pet godina? Kako ćemo meriti napredak i vrednost naših napora?
Kako to da postignemo?	Akcioni plan koji opisuje sledeće akcije koje će se preduzeti kako bi se moglo doći do tamo gde organizacija želi da bude, pokrivajući tri elementa, a to su: ljudi, procesi i tehnologija. Koji specifični alati i procesi će se koristiti? Kako ćemo motivisati ljude da promene svoje prakse? Kako razviti prateću tehnološku infrastrukturu?

Kako bi mogla biti uspešna, strategija menadžmenta znanja ne može samo utvrditi ciljeve, kao što je: „postati organizacija koja uči". Isto tako, ona treba da odredi ključne potrebe i probleme unutar kompanije, kao i da omogući okvir za njihovo rešavanje. Zbog toga strategija menadžmenta znanja mora da bude tesno povezana sa *SWOT* analizom kompanije – njenom misijom, ciljevima, potrebama, kao i vrednostima i načinom rada. Važno je razumeti te elemente pre nego što se počne sa razvijanjm strategije za kompaniju.

Svaka strategija treba da da odgovore na tri sledeća pitanja:

- Gde se trenutno nalazimo?
- Gde želimo da budemo?
- Kako to da postignemo?

Strategija menadžmenta znanja može se formirati oko tih pitanja i uključiti elemente koji su opisani u tabeli 4.

Navedena pitanja možemo postaviti na drugačiji način pre nego što počnemo sa pripremom strategije menadžmenta znanja za kompaniju (tabela 5).

Tabela 5. *Mogući rezultati primene strategije menadžmenta znanja*
Izvor: [59]

Koje znanje želimo da delimo?	Koju vrstu znanja i kakav kvalitet znanja želimo da delimo?
S kime želimo da delimo znanje?	Kome će znanje biti namenjeno? Ko bi trebalo da koristi to znanje?
Na koji način će se deliti znanje?	Koji će se kanali koristiti za deljenje znanja?
Zašto će se to znanje deliti?	Šta motiviše ljude za deljenje znanja? Kakve ciljeve želimo da postignemo?

Davanje odgovora na ova pitanja nije sve što je neophodno učiniti. Kompanija treba da pripremi dokument koji definiše njenu strategiju menadžmenta znanja.

Tabela 6. *Mogući rezultati primene strategije menadžmenta znanja*
Izvor: [59]

Abstrakt	Abstrakt sadržaja dokumenta na najviše 1–2 stranice papira
Pozadina	Opis načina na koji je strategija povezana s drugim korporativnim planovimai aktivnostima.
Poslovni slučaj	Definicija upravljanja znanjem unutar organizacije. Utvrđivanje potencijalnih dobiti za organizaciju. Objašnjenje doprinosa koji će upravljanje znanjem dati organizaciji i osvrt na ključne ciljeve organizacije. Taj deo strategije je ključan za obezbeđivanje usklađenosti između ključnih ciljeva organizacije i upravljanja znanjem.
Postojeća situacija	Informacije o sprovedenim aktivnostima upravljanja znanjem (uključujući nekestvarne primere dobre prakse) i iskustvima, odnosno dobitima i preprekama za budući napredak. Informacije o ključnim tačkama iz revizije znanja. Informacije o područjima u kojima neodgovarajuće upravljanje znanjem stvara probleme i poslovnu neučinkovitost.
Izazovi učesnika i potrebe za znanjem	Abstrakt ključnih pitanja i potreba organizacije za znanjem između članova organizacije i učesnika.
Vizija upravljanja znanjem	Sažeti opis (1–2 rečenice) načina na koji će upravljanje znanjem igrati važnu ulogu u organizacijskim aktivnostima u narednih pet godina.
Pregled strategije	Prezentacija aktivnosti i projekata koji će se implementirati, grupisati u određene teme ili područja aktivnosti, kao što su: alati i metode upravljanja znanjem; ko će posedovati i sprovoditi strategiju; pomeranje strategije itd.
Akcioni plan	Informacije o ciljevima, vremenskim rokovima, resursima i traženim proračunima za sve akcije.
Zavisnosti	Informacije o ključnim zavisnostima, kao što su: dostupnosti ključnih zaposlenih,odobrenje proračuna itd.
Zaključci i detaljni koraci	Opis onoga što se mora zatim izvršiti kako bi se strategija pretvorila u akciju.
Dodatak	Npr. neki materijali o upravljanju znanjem, kao što su definicije postojećeg projekta i inicijative.

Dobra strategija menadžmenta znanja treba da se bazira na tri elementa: jednostavnost, produktivnost i standardizacija. Prilikom planiranja strategije menadžmenta znanja veoma je važno obratiti pažnju na sve te ključne aspekte, jer svaka strategija koja ih ne uključi osuđena je na neuspeh. Dobra strategija treba da uravnoteži dugoročnu viziju kratkoročnih rešenja (engl. *quick wins*), odnosno da odražava ravnotežu između brzih rezultata i dugoročno održivog menadžmenta znanja.

2.4 Ekonomija znanja

Još uvek u potpunosti ne postoji razumevanje kako se znanje ponaša kao ekonomski resurs. Nema dovoljno iskustva za formulisanje teorije po ovom pitanju kao i provere. Za sada možemo jedino da zaključimo da je potrebna jedna takva ekonomska teorija koja treba da postavi znanje u središte procesa proizvodnje bogatstva u kompaniji. Samo takva teorija može da objasni sadašnju ekonomiju i privredni rast, kao i inovacije. Ali, u isto vreme može da objasni zašto su neke nove kompanije na svetskom globalnom tržištu, naročito u područjima visokih tehnologija u trenutku izbacile sa tržišta sve svoje konkurente.

Razni autori koji se bave definisanjem ključnih karakteristika ekonomije znanja dolaze do zajedničkog stava da su glavni pokretači ekonomije znanja: globalizacija, znanje

i intelektualni kapital, razvoj informacione tehnologije i promene sa svom svojom kompleksnošću. [62] Promene sistema vrednosti u svakodnevnom životu i promena načina razmišljanja ljudi u ekonomiji direktno je povezano za pomeranje (engl. *shift*) od industrijske ekonomije ka ekonomiji znanja. Osnovna karakteristika ekonomije znanja je da su ekonomski razvoj i promene na tržištu ekstremno brze i nepredvidive. Ključni nosioci ekonomije znanja nisu više industrijske već inovativne kompanije koje svoj rad zasnivaju na znanju. Danas, ključni faktor uspeha ne predstavlja kapital već sposobnost, ljudi i znanje kompanije. Računarski dizajn i *e-busines* zamenjuje automatizacija. Važno je kontinuirano učenje, jer danas više nije važno šta se zna, već koliko brzo nešto može da se nauči. Saradnja i timski rad zauzimaju ključno mesto u kompanijama, dok se zaposleni posmatraju kao investicija. [62]

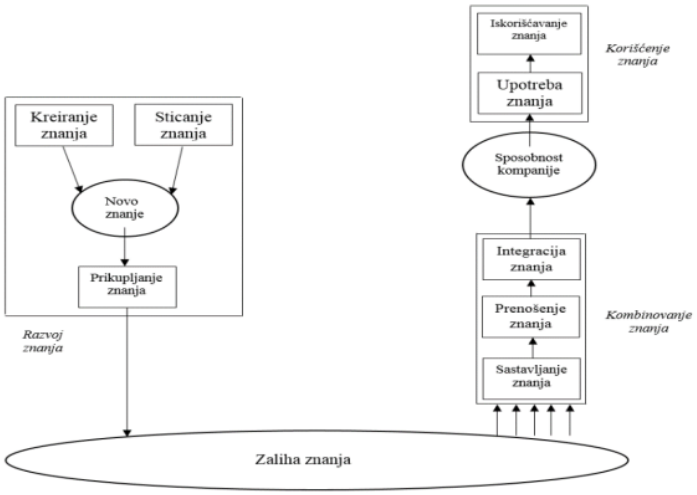
Kada se razmatra poslovanje savremenih kompanija u ekonomiji znanja jasno se uočavaju dve pojave: preorijentacija od proizvoda ka uslugama i posmatranje znanja kao proizvoda. [63] Ekonomija znanja posmatra znanje kao proizvod jer znanje koje poseduje kompanija, ona koristi i kombinuje na kreativan i nov način. Time se podstiče inovacija na svim nivoima kompanije i omogućava pružanje usluga sa dodatnom vrednošću za korisnike usluga. Kako bi se ostvarila konkurentska prednost i kompanija bila uspešna u ekonomiji znanja, potrebno je da znanje stalno uvećava svoju vrednost, tj. da poseduje *KnoVa* – faktor vrednosti znanja (engl. *The KnoVa – knowledge value*). [63]

2.4.1 Prednosti primene menadžmenta znanja

Prema određenim predviđanjima razvoj malih i srednjih kompanija će biti ključni faktor uspeha širom sveta u budućim decenijama. [64] U malim i srednjim kompanijama koje su orijentisane na inovacije i brzi razvoj zahteva se ubrzana primena znanja, kao i znanja kojima se upravlja na produktivan, efektivan i bezbedan način [65]. U suštini znanje postaje roba koja nudi konkurentsku prednost svake kompanije. Da bi zadržale konkurentnost na tržištu, kompanije moraju imati određeno znanje, koje moraju znati uskladiti i iskoristiti, i to u što kraćem vremenskom roku. [66].

Prema tvrdnjama Egbua i Leeja snage malih i srednjih kompanija se ogledaju u: manjim formalnim strategijama. Neformalna mreža unapređuje posvećenost zaposlenih i njihovo prihvatanje menadžmenta znanja. Brži je odgovor na promenjive zahteve tržišta i znanje potrebno za zadovoljavanje potreba tržišta. [66][67] Nedovoljna sposobnost finansiranja dugoročnih i rizičnih programa menadžmenta znanja, kao i slabosti u specijalizovanim područjima tehnološke kompetencije, nesposobnosti ulaganja u obrazovanju i usavršavanju glavnie su slabosti malih i srednjih kompanija [66][67]. Ostale slabosti se ogledaju u činjenici da one imaju malo iskustva u području menadžmenta, neuravnotežen odnos snaga ukoliko pokušaju da sarađuju sa velikim kompanijama, poteškoće u implementaciji složenih zakonskih propisa, kao i troškova usklađivanja s njima.[68]

Problemi informacionih sistema u današnjim uslovima poslovnja prelaze iz područja menadžmenta informacijama u područje menadžmenta znanja. Kako bi bile konkurentne, male i srednje kompanije koriste menadžment znanja za upravljanje svojom kompetetnošću kao najdragocenijom imovinu svake kompanije [64][69].



Slika 7. *Dinamična sposobnost kompanije – odnos između menadžmenta znanja i sposobnosti kompanije*
Izvor: [71]

McAdam i Reid uočili su određene razlike od menadžmenta znanja malih i srednjih kompanija. Prema njihovim tvrdnjama oblast malih i srednjih kompanija je manje napredna u pogledu izgradnje znanja, jer je njihov pristup više mehanički, dok se manje oslanjaju na društvenu interakciju. [70]

U istraživanjima koja je sproveo Beijerse, otkrio je da ne postoji eksplicitno pravilo usmereno ka strateškom menadžmentu znanja[72]. Corso i saradnici, u svom istraživanju naglašavaju da su male kompanije sklone da stave veće težište na menadžmentu tacitnog znanja nego velike kompanije, kao i to da su kanali za komunikaciju u malim i srednjim kompanijama češći između kompanija nego unutar samih kompanija [73]. Neka istraživanja bavila su se primenom informacionih i komunikacionih tehnologija (engl. *ICT*) u menadžmentu znanja u malim i srednjim kompanijama. Rezultati su pokazali da su malim kompanijama nedostajali finansijski izvori i kvalifikovana radna snaga, kao i kompetetnost za upravljanje vremenom kako bi kompanije mogle da ulažu u napredne informaciono-komunikacione tehnologije [74]. Neki autori, kao što je Salojarvi, tvrde da kompanije koje sistematično primenjuju sistem, rastu brže od kompanija koje nemaju strategiju i praksu menadžmenta znanja.[74][75] Prema O'Dellu, promenila se poslovna logika u kompanijama koje primenjuju najbolje prakse kroz sprovođenja inicijative menadžmenta znanja.[76] Najčešće promene su: smanjenje troškova, ponovna upotreba znanja i naučenih lekcija, brzina, inovacije, ponovna upotreba znanja i iskustva (engl. *know-how*) menadžmenta znanja, brendiranjai diferencijacije, kao i unapređenje kvaliteta znanja.[74]

2.4.2 Prepreke i poteškoće u menadžmentu znanja

Postoje mnoge prepreke i poteškoće u realizaciji menadžmenta znanja. U istraživanju koje je sproveo Saaristo 2012. godine, prepreke u primeni menadžmenta znanja u kompanijama su:[7]

- manjak razumevanja koncepta menadžmenta znanja i njegovih prednosti,
- problemi prilikom određivanja vrste znanja kojim se upravlja, kao i njegove

dostupnosti,

- savladavanje tehnoloških ograničenja,
- nedostatak kompetetnosti u području tehnologije,
- nedostatak tehnoloških resursa,
- nedostatak programa osposobljavanja,
- finansijska ograničenja,
- izostanak učešća zaposlenih,
- nedostatak poverenja i izostanak sistema nagrađivanja za deljenje znanja,
- nespremnost zaposlenih za deljenje znanja,
- vremenski zahtevna i preskupo sprovođenje menadžmenta znanja.[7]

Određeni autori su identifikovali još neke nedostatke. Wunram tvrdi da prepreke uključuju sve što je vezano uz ljudska, organizaciona i tehnološka pitanja, a što ograničava menadžment znanja [77]. Male i srednje kompanije su slabe u području specifičnih tehnoloških kompetencija. [66] Pored toga, nedostatak strategija za sticanje znanja, odnosno jasnih strategija menadžmenta znanja koje sprovode, kao i nedostatak utvrđivanja odgovornosti mo predstavljati problem za kompanije. Veoma često zaposleni nisu svesni procesa sticanja znanja i često traže brza rešenja u poslu s ciljem rešavanja problema, a ne uzroka, propuštajući tako priliku da zabeleže iskustva i prenesu znanje ostalim zaposlenima. Male i srednje kompanije su možda svesne snage menadžmenta znanja i važnosti sticanja znanja unutar svoje kompanije, smatrajući da imaju važnije prioritete i potrebe [66].

Postoji i prepreka krađe ideja. Još jedna prepreka odnosi se i na pronalaženje vremena za sticanje znanja. Zaposleni su previše opterećeni i proces sticanja znanja može biti u sukobu sa njihovim obave na [66]. Ispitanici u kompanijama koje poseduju strategiju menadžmenta znanja smatraju preopterećenje informacijama, nedostatak vremena za deljenje znanja i nekorišćenje tehnologije za deljenje znanja manjim problemima u odnosu na ispitanike u kompanijama bez strategije menadžmenta znanja [74]. Proces prikupljanje kvalitetnog sadržaja iz celokupne kompanije u svrhu popisivanja znanja pred vlja težak posao, dok su za pretvaranje implicitnog znanja u eksplicitne informacije potrebne posebne veštine, a često i kreativnost.

Projekti menadžmenta znanja su veoma rizični poduhvati. Brojne kompanije započnu projekat, ali kasnije odustanu od njega. Postoje različiti razlozi koji uzrokuju propadanje projekata. Pored dovoljnog vremena za zadatke menadžmenta znanja, jednostavnih alata za upotrebu, jedan od najvažnijih činilaca je učešće zaposlenih unutar kompanije. Ako zaposleni ne učestvuju u njima, oni su osuđeni su na neuspeh. Učestvovanje zaposlenih u projektu je tesno povezano sa njihovom motivacijom. Iz tog razloga odgovorni menadžer u projektu menadžmenta znanja mora da se suoči sa pitanjem na koji način uključiti i motivisati zaposlene u kompaniji.

3. Menadžment znanja

U skladu sa dinamičnim razvojem informacionih tehnologija menadžment znanja (engl. *knowledge management – KM*) danas nudi izazove i mogućnosti više nego ikada ranije. To je razlog zbog čega, danas, ključnu ulogu imaju IT stručnjaci koji raspolažu znanjem i veštinama upravljanja i korišćenja određenih informacija, i imaju pristup najznačajnijim izvorima informacija.

3.1 Definicija menadžmenta znanja

Nedostatak univerzalne definicije kategorije znanja rezultovao je u mnoštvo mogućih pristupa objašnjavanja menadžmenta znanja. Dodatni problem je i neusaglašenost oko toga šta predstavlja menadžment znanja – da li je to koncept, neki strategijski alat, poslovna praksa ili nešto drugo.

Ako predpostavimo da su informacije glavni faktor za konstituisanje znanja, Crager i Lemons definišu menadžment znanja kao sistematski proces pronalaženja, izbora, organizacije, pripreme i prezentovanja informacija na način koji poboljšava razumevanje zaposlenih u specifičnim sferama interesovanja. Postoje aktivnosti u okviru menadžmenta znanja koje pomažu fokusiranje kompanije na prikupljanje, čuvanje i upotrebu znanja u svrhu rešavanja problema, dinamičkog učenja, strategijskog planiranja i donošenja odluka. Cilj menadžmenta znanja treba da bude poboljšanje performansi kompanije i pojedinaca kroz identifikaciju, osvajanje, validaciju i transfer znanja [78]. Stratfild i Vilson navode da se znanjem ne može upravljati, već samo informacijama i znanjem koje imaju zaposleni u određenim institucijama. Čak i tada, upravljanje je nepotpuno jer se granice ljudskog znanja neprekidno pomeraju. [79] Seiner daje definiciju menadžmenta znanja kao *koncepta prema kome kompanija vrši prikupljanje, organizaciju, deljenje i analizu znanja pojedinaca i grupa širom kompanije na način na koji ono direktno utiče na uspešnost poslovanja*. [80] Po Levinsonu, putem menadžmenta znanja *kompanije stvaraju vrednost iz svoje intelektualne imovine, kao i imovine utemeljene na znanju*. [81] Drugu definiciju menadžmenta znanja predstavio je Sveiby koji navodi da se *menadžment znanja zasniva na prepoznavanju i analiziranju raspoloživih i neophodnih resursa znanja i procesa a sve u cilju ispunjavanja organizacionih ciljeva* [82]. Villegas pak definiše menadžment znanja kao *jednostavan prenos znanja s jedne osobe na drugu, čiji rezultat omogućuje korisniku da upotrebi prikupljenu mudrost iskusnijih članova neke organizacije ili grupe*. [83] Estacio tvrdi da je menadžment znanja *logički sistem koji omogućava organizaciji da sadržajno ostvari svoje ciljeve na osnovu sposobnosti pretvaranja prećutnog i eksplicitnog znanja u navike, bolje planiranje i upotrebu*.[84]

Murray i Myers menadžment znanja uglavnom definišu kao sticanje, diseminaciju i korišćenje znanja unutar kompanija koji obuhvata i procese učenja, i upravljanje informacionim sistemima ili, preciznije, sistematsko upravljanje aktivnim znanjem, kao i procesima njegovog stvaranja, akumuliranja, organizovanja i korišćenja. Potrebno je individualno znanje integrisati u kolektivno koje je moguće kasnije distribuirati i koje će unutar organizacije biti adekvatno primenjeno.[85] Malhotra tvrdi da menadžment znanja zadovoljava kritične parametre prilagođavanja kompanije, preživljavanja i kompetentnosti pred narastajućim naglim promenama u njenom okruženju. Suštinski, menadžment predstavlja organizacione procese koji zahtevaju sinergijske kombinacije podataka i mogućnosti procesuiranja informacija primenom informacionih tehnologija i kreativne i

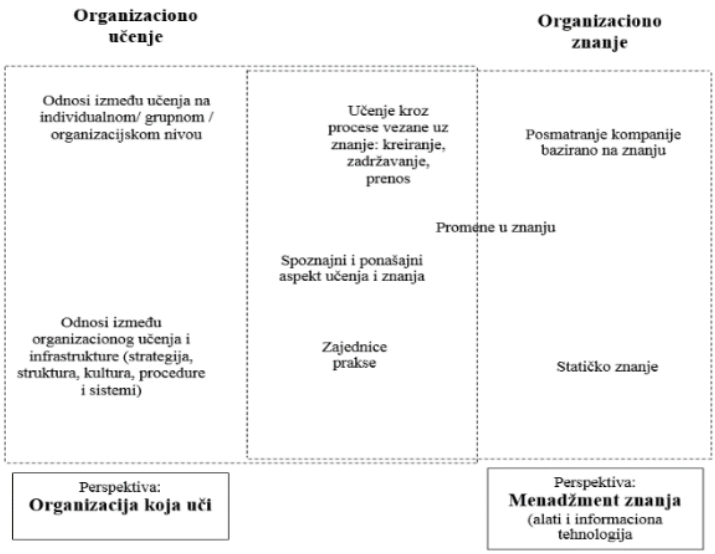
inovativne sposobnosti ljudskih bića. [86] Po Skyrme-ju, menadžment znanja predstavlja eksplicitno i sistematično upravljanje vitalnim znanjem primenom odgovarajućih procesa: kreiranje, prikupljanje, organizacija, raspodela, korišćenje i eksploatacija. Ono zahteva prelazak personalnog znanja u korporativno koje može biti pristupačno kroz kompaniju i prikladan način primenjeno. [87] Bock definišući menadžment znanja kaže da je to način na koji kompanije kreiraju, čuvaju i ponovo upotrebljavaju znanje da bi ostvarile svoje ciljeve. [88] *Knowledge point* vidi menadžment znanja kao sistematični proces pronalaženja, izbora, organizovanja, prečišćavanja i prezentovanja informacija na način koji unapređuje kompetencije zaposlenih u oblasti od interesa. [89] Iz svega prethodno navedenog, proizilazi da je menadžment znanja sistematski i organizaciono specifičan proces koji se odnosi na prikupljanje, organizovanje i razmenu znanja zaposlenih kako bi ga drugi zaposleni mogli koristiti zbog poboljšanja efektivnosti i produktivnosti rada, što je u skladu sa tvrdnjama Alavija i Leidnera. [90]

3.2 Koncepti menadžmenta znanja

Kompanije svoj uspeh postižu kroz adekvatno obrazovanje zaposlenih, znanja i inteligencije, talenta i situacionog faktora sreće. Obzirom da uslovi privređivanja postaju sve dinamičniji, kompanije moraju brže da uče ukoliko ne žele da nestanu u uslovima stalne konkurencije. Individualno i timsko učenje nije dovoljno, već je potrebno kolektivno i organizovano učenje i znanje. Savremeni koncepti menadžmenta znanja su:[91]

- kompanija koja uči,
- jezgro kompetentnosti,
- menadžment znanja (engl. *Knowledge Management – KM*),
- *Total Quality Management – TQM*,
- *Downsizing*,
- *Outsourcing*,
- reinženjenring poslovnih procesa,
- *Benchmarking*,
- strategija kao revolucija,
- *Patching*,
- *Enterprise Resources Planning – ERP*,
- *Balanced Scorecard – BSC*,
- *E-commerce*.

Ovi koncepti menadžmenta znanja nastali su kao odgovor na izazove menadžmenta 21. veka. Oni predstavljaju menadžment paradigme koje su kreirane uglavnom u poslednjih 15 godina. [91] Koncept menadžmenta znanja stvoren je i razvija se na konceptu „organizacije koja uči", „jezgra kompetentnosti" i „TQM".



Slika 8. *Koncepti povezani sa menadžmentom znanja*
Izvor: [92]

Detaljna identifikacija veza i odnosa gore navedenih koncepata i menadžmenta znanja predstavlja veliki istraživački poduhvat što prevazilazi okvire ovog rada, ali se nadamo da ćemo na ovaj način pokrenuti diskusiju u naučnoj i stručnoj javnosti, što je i osnovni cilj navođenja ovih koncepata.

3.2.1 Intelektualni kapital

Sistemsko prikupljanje i korišćenje znanja postiže se kreiranjem odgovarajućeg okruženja koje podstiče deljenje i transfer znanja i kreiranje nove vrste korporativne imovine – intelektualnog kapitala. Pojavom i razvojem savremenih oblika organizovanja kompanija u prvi plan pojavljuje se znanje kao najvažniji resurs. Znanje se može razmatrati i kao *input* i kao *output* kompanije [93]. Intelektualni kapital kompanije, u čijoj je osnovi znanje, predstavlja njenu nevidljivu imovinu i veoma je važan deo njene ukupne tržišne vrednosti. Danas u kompanijama vrednost nevidljive imovine, može biti višestruko veća od vrednosti materijalne imovine.[94] Intelektualni kapital kompanije sadrži brojne elemente, koji su u neprestanoj međusobnoj interakciji, a koji su vezani za tržište, strukturu kompanije i čoveka kao najvažnijeg činioca koji poseduje znanje. Takođe, intelektualni kapital možemo posmatrati i kao osnovu efektivne upotrebe resursa za kreiranje zadovoljavajuće vrednosti za kompaniju i njene partnere.

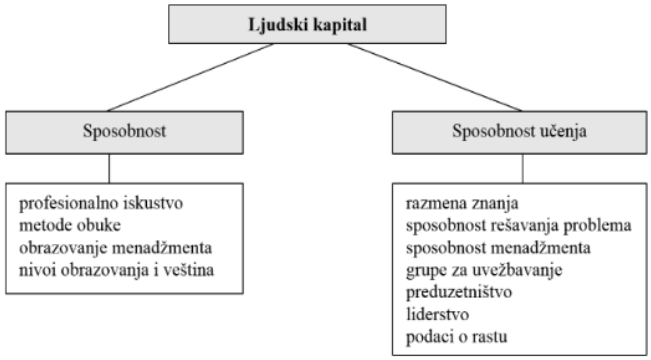
Da bi stvorili vrednost kompanije neophodno je postojanje veze između sastavnih elemenata intelektualnog kapitala, tj. između ljudskog, strukturnog i relacionog kapitala. Kreiranje vrednosti dolazi u slučaju međusobne razmene znanja između tri elementa intelektualnog kapitala, i u velikoj meri utiče na neprekidan razvoj organizacionih sposobnosti, dok razmena znanja olakšava i ubrzava učenje. Nužno je kontinuirano unapređivanje samih strukturnih elemenata, kao i stvaranje protoka znanja između njih.[95]

Intelektualni kapital podrazumeva sva znanja koja poseduju zaposleni u nekoj kompaniji – ljudski resursi. To je pre svega intelektualni materijal koji doprinosi stvaranju

bogatstva. [96] Ovakav kapital je težak za identifikaciju, a još teži za efikasan razvoj [97] Današnja ekonomija primenjuje tzv. neopipljiv kapital koji se sastoji od ugleda, robnih marki, tradicije, odnosa sa kupcima, povezanosti sa partnerima, iskustvima i veštinama u poslovanju, ali i u znanju i sposobnosti zaposlenih. Danas ti pokazatelji stvaraju mnogo više novih vrednosti u odnosu na tradicionalne pokazatelje.

Savremene kompanije ulažu napore da dovedu u vezu znanje zaposlenih sa finansijskim rezultatima kompanije. Na taj način se dolazi do termina intelektualni kapital koji se odnosi na ukupnu intelektualnu svojinu i intelektualni potencijal koji kompanija koristi za stvaranje nove vrednosti. Ovaj kapital čini akumulisano znanje koje neka kompanija poseduje u svojim zaposlenima, postupcima, patentima, dizajnima i vezama i istovremeno predstavlja znatno širi pojam od znanja. [98] Znanje i intelektualni kapital predstavljaju trajne resurse obezbeđivanja konkurentske prednosti kompanija.[99]

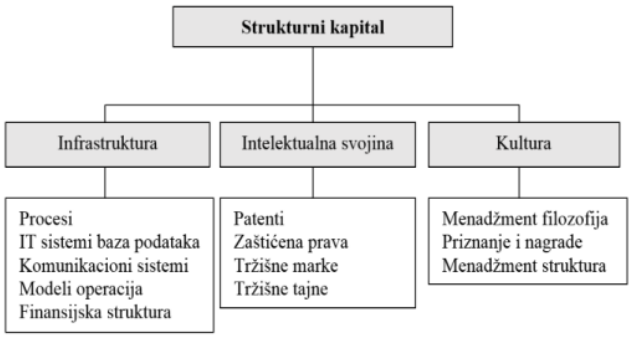
Spremić u svojim istraživanjima tvrdi da je ostvarivanje veće tržišne vrednosti kompanije u korelaciji sa kvalitetom i kvantitetom finansijskog kapitala, dok poslednjih dvadesetak godina ispoljava i vezu sa visinom intelektualnog kapitala i sinergije između njegovih strukturnih segmenata – ljudskog, strukturnog i klijentskog kapitala. [100]



Slika 9. *Komponente ljudskog kapitala*
Izvor: [100]

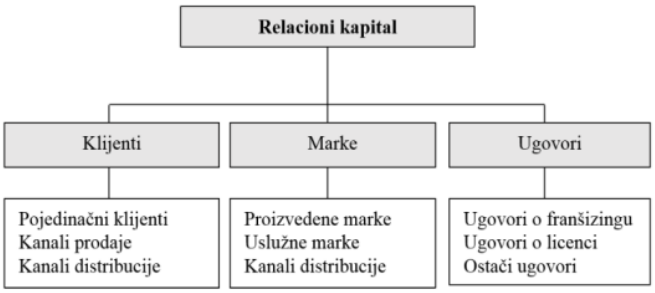
Današnja ekonomija ljudski kapital svrstava kao noseći stub intelektualnog kapitala i osnovnu vrednost svake kompanije. To je pokretačka snaga intelektualnog kapitala i predstavlja osnovu tržišne vrednosti poslovnih subjekata, naročito u intelektualno intenzivnim industrijskim granama.[101]

Strukturni kapital predstavlja vlasništvo poslovnog subjekta i pomaže mu kao logistička podrška i pokretač pretvaranja ljudskog kapitala u produktivnu vrednost. Takođe, predstavlja i sposobnost kompanije da koristii potencijal svojih zaposlenih na inovativan način. Najčešće se karakteriše kroz primenu informacionih tehnologija, veština i iskustva koje kompanija ugrađuje u procese i sisteme. On predstavlja recepte znanja kojima drugi zaposleni mogu povećati vrednost za dobit kompanije.



Slika 10. *Komponente strukturnog kapitala*
Izvor: [100]

Relacioni (klijentski) kapital nastaje sjedinjavanjem kompanije sa njenim okruženjem, najpre negovanjem pozitivnih odnosa sa svojim kupcima i dobavljačima. Poseduje ogroman značaj zbog činjenice da sadrži vrednost relacija, sve odnose i veze s klijentima, poslovnim partnerima, kupcima, dobavljačima, segmentima tržišta, lojalnošću i snagom. Kompanije moraju da uzmu u obzir činjenicu, da kvalitet koji pružaju bude iznad, ili jednak kvalitetu koji potrošač očekuje.[102]



Slika 11. *Komponente relacionog (klijentnog) kapitala*
Izvor: [103]

Možemo zaključiti da intelektualni kapital predstavlja kombinaciju ljudskog kapitala i strukturalnog kapitala. Predstavlja mogućnost da se znanje i apstraktna dobra pretoče u izvore bogatstva, umnožavajući ljudski kapital strukturnim kapitalom. [104] Iako je znanje o postojanju i važnosti intelektualnog kapitala u stalnom porastu, on još uvek predstavlja nemerljivu stavku za većinu kompanija.

3.2.2 Menadžment znanja i intelektualni kapital

U svim oblastima poslovanja potreba za znanjem nije ista. Obezbeđivanje najnovijih znanja i njihov transfer donosiocima odluka, u svrhu poboljšanja efikasnosti kompanije, predstavlja cilj menadžmenta znanja.[105] Imajući u vidu, da kompanije ne mogu u perspektivi svoje poslovanje zasnivati na istim informacijama i znanjima, javlja se potreba za njihovom neprestanom inovacijom. Svaka kompanija treba da stvara bazu najaktuelnijih znanja koju će neprestano da inovira. Danas se sve više pojavljuju kompanije koje kreiraju, stvaraju i koriste znanje.

Menadžeri u Srbiji ne koriste u velikoj meri raspoloživa nova znanja i intelektualni kapital u kompanijama. Uglavnom se baziraju na postojeća znanja i ne izražavaju

motivaciju za primenom novina. Suprotno tome menadžeri iz zapadnih zemalja u razvijenim ekonomijama veliki deo svog radnog vremena posvećuju učenju i usavršavanju. Primena novih modela poslovanja zahteva i promene u primeni znanja iintelektualnog kapitala. Dinamika modernog poslovanja mnoge menadžere postavlja u položaj posmatrača jer nisu u stanju da slede nove trendove. Kvalitativni pokazatelji, zadovoljstvo zaposlenih, produktivnost procesa i mogućnosti unapređenja za njih ne predstavlja prioritet.

Od intelektualnog kapitala mogu se dobiti višestruke koristi. Adekvatno upravljanje intelektualnim kapitalom može dovesti do povećane sposobnosti, kreiranja nove dodate vrednosti koja daje doprinos uvećanoj vrednosti same kompanije. Na taj način se postiže efikasnije korišćenje potencijala, unapređuju poslovni procesi, mnogo efikasnija postaje upotreba ljudskog kapitala. Zaposleni imaju veću motivisanost i komunikacija unutar kompanije je kvalitetnija. Sve to dovodi do unapređenja ugleda kompanije, potrošači postaju zadovoljniji, a samoj kompaniji se znatnije povećava tržišna vrednost.[106]

Ovde se može izvesti zaključak da je oslanjanje na unutrašnje resurse, tj. znanje zaposlenih osnova za postavljanje moderne strategije poslovanja u turbulentnim tržišnim uslovima u kojima kompanije posluju. Izvesno je da budućnost pripada deljenju znanja, odnosno, razmeni znanja u tržišnom smislu. Za razliku od ostalih resursa, razmena znanja jedna je od najvažnijih karakteristika, jer sa upotrebom znanja njegova vrednost neprekidno raste.

3.2.3 Znanje kao nevidljiva imovina kompanije

Znanje koje poseduju zaposleni u kompaniji može se posmatrati i kao nevidljiva imovina. Sveiby je predložio primenu monitora neopipljive vrednosti (engl. *Inagible Assets Monitor*) kako bi podstakao menadžere da eksperimentišu sa njenim predstavljanjem.[107] On se može klasifikovati u tri kategorije:

- individualne sposobnosti – predstavljaju ljudski potencijal da deluju u različitim situacijama (uključuje veštine, obrazovanje, iskustvo, vrednosti, socijalna umeća);
- interna struktura – čine je patenti, koncepti, modeli, računarski i administrativni sistemi;
- eksterna struktura – čine je veze sa korisnicima i dobavljačima, brendovima, ugledom.

Ova kategorizacija kao i Konradova teorija [107] o merenju neopipljivih vrednosti razvijena je od strane Švedske radne grupe 1987. godine, a objavljena u izveštaju 1988. godine. Za potrebe menadžmenta ona se dalje razvija pod nazivom „Monitor neopipljive vrednosti" od strane Sveibija [108]. Sve vrednosti i strukture rezultat su aktivnosti ljudi. Ako menadžeri uspeju da pravilno usmere napore svojih zaposlenih moći će ranije da izvrše kreiranje nevidljive strukture i time poboljšaju svoje poslovne procese. Zaposleni u komaniji mogu da koriste svoje kompetencije u dva osnovna pravca: spoljni pravac (radeći sa korisnicima usluga) i unutrašnji pravac (gradeći organizaciju).

Znanje kao nevidljiva imovina se u poslednje dve decenije pojavljuje kao glavni faktor u kompanijama. Vrednost kompanije danas se ne ogleda samo u njenoj fizičkoj imovini, već se njena vrednost bazira na znanju, iskustvu i intelektualnoj imovini, što se pak sve zasniva na ljudima. [108] Takve kompanije se danas nazivaju „inteligentne organizacije", „organizacije znanja" i „organizacije koje uče".

3.3 Elementi menadžmenta znanja

Vodeći mislilac i praktičar u oblasti upravljanja znanjem Ruggles, definisao je sledeće elemente – integralne komponente menadžmenta znanja: [109]

- stvaranje novog znanja,
- upravljanje korisnim znanjem iz eksternih izvora,
- primena raspoloživog znanja za donošenje odluka,
- implementacija znanja u procese, proizvode i/ili usluge,
- prikaz znanja u dokumentima, bazama podataka i softverima,
- lako širenje znanja u vidu organizacione kulture i inicijative,
- prenošenje postojećeg znanja u druge delove organizacije i
- ocena vrednosti znanja i/ili uticaja upravljanja znanjem.

Koncept menadžmenta znanja pretpostavlja mogućnost i potrebu da se upravlja eksplicitnim i implicitnim znanjem kompanije, sa svrhom da se dođe do inovacije, koja je ključ opstanka i uspeha. Značaj primene ovog koncepta u kompanijama je u činjenici sve većeg značaja intelektualnih resursa kompanija u novim trendovima ekonomije. Da bi se upravljalo znanjem kao resursom, neophodna su tri elementa:[110]

- ljudi i odgovarajuća organizaciona kultura,
- procesi promena i
- primena informacionih i drugih tehnologija.

Menadžment znanja, podrazumeva proces koji ima sledeće elemente: [111]

- analiza trenutnog znanja kao resursa u kompaniji,
- identifikacija ciljeva za generisanje, zaštitu i primenu novog znanja,
- prenos, razmena i širenje znanja i
- efikasno korišćenje znanja i merenje (kontrola) „performansi i vrednosti”

znanja kao resursa.

Pod stvaranjem znanja podrazumeva se proces pronalaženja znanja iz eksternog okruženja i stvaranje novih znanja u okviru poslovnog sistema. Znanje se može osigurati iz spoljnih izvora – nabavkom tehnologije (licence), nabavkom softvera, zapošljavanjem eksperata, strategijskim partnerstvima i korišćenjem konsultanata.[112] Generisanje znanja odvija se kroz proces individualnog i organizacionog učenja. Ovaj pristup generisanju znanja podrazumeva da menadžment stimuliše učenje svakog pojedinca i međusobnu razmenu znanja. Posebno važan problem je obezbediti koordinaciju članova kolektiva koji imaju različito znanje, a koje ipak može biti komplementarno, tako da u toj kombinaciji i interakciji, mogu proizvesti novo, specijalizovano znanje ili dovesti do kreiranja organizacionih sposobnosti. A onda, od njih kreirati i organizacione kompetencije, pa njihovim povezivanjem, stvarati i ključne kompetencije kompanije.

Razmena znanja je i jedan šire shvaćeni proces koji omogućava da se znanje širi kroz veći deo ili kroz ceo poslovni sistem. Kako bi znanje moglo da se primeni za razvoj kompanije, treba da važi pravilo da je moć u razmeni znanja. Najvažniji faktor stimulacije

razmene znanja je podsticaj na inovativnost, kreativnost i poverenje. Razmena znanja se može sprovesti neformalnim i formalnim procesima (sastanci, seminari, kreativne radionice, formiranje baze podataka i interne dokumentacije). [112]

Smatra se da je generisanje znanja u kompanijama proces koji vodi ka formiranju organizacionih sposobnosti. Kreirane sposobnosti, na osnovu resursa znanja različitih ljudi u kompaniji, kao i u kombinaciji sa ostalim materijalnim resursima, čine osnovu organizacionog znanja. Generisanje znanja kroz proces organizacionog učenja ne svodi se na individualno učenje i povezivanje znanja pojedinaca, već se širi na celu organizacionu strukturu.

Menadžment znanja podrazumeva determinisanje strategije, metoda generisanja znanja i tehnologija za produktivno korišćenje intelektualnog kapitala s ciljem unapređenja konkurentnosti. On uključuje i integrisani pristup identifikaciji, upravljanju i deljenju svih informacionih resursa kompanije. [113] Kreiranje i korišćenje znanja zahteva transfer individualnog znanja zaposlenih u organizaciono znanje. Menadžment znanja može doprineti uvećanju vrednosti i konkurentnosti, unapređivanjem njegove povezanosti i inoviranjem.[112] Povezivanje znanja o najboljim praksama, ogleda se u menadžmentu znanja koje cirkuliše između poslovnih jedinica radi postizanja sinergijskih efekata na nivou kompanije. Inovacija procesa/proizvoda i povećanje konkurentske sposobnosti kompanije može se realizovati kombinovanjem postojećeg i/ili kreiranjem novog znanja.

Savremeno poslovanje ne iziskuje samo znati nešto o poslovnoj akciji ili posedovati vrednu informaciju, već je važno i znati na koji način iskoristiti skup informacija u specifičnoj tržišnoj situaciji. Organizaciono znanje može da bude identifikovano i valorizovano kroz korišćenje ili transfer, samo ako je uključeno ili uklopljeno u sistem, proces, proizvod i organizacionu kulturu. Znanje kao organizacioni resurs treba što efektivnije i efikasnije koristiti sa ciljem da se ostvare mnogobrojni benefiti za kompaniju, koji se ogledaju u ostvarivanju boljih poslovnih rezultata, kreiranju inovacija, stvaranju organizacionih sposobnosti, uvećanju sposobnosti organizacionog učenja i dr. Uslov da bi se ovo postiglo, neophodno je prethodno u kompaniji ostvariti efektivan i efikasan proces i sistem menadžmenta znanja.

3.4 Modeli menadžmenta znanja

Da bi koncept menadžmenta znanja imao svoju adekvatnu primenu i pružio svoj puni doprinos potrebne su jake teorijske osnove. U literaturi [114] zavisno od osnovnih elementa menadžmenta znanja predstavljeni su različiti modeli. [115] Autori najpoznatijih modela su: Beer (1984)[116], Wiig (1993)[117], von Krogh i Roos (1995)[118], Nonaka i Takeuchi (1995)[46], Boisot (1998)[119], Choo (1998)[120] i Bennet i Bennet (2004)[121]. Dalje će u radu ukratko biti predstavljeni neki od navedenih modela menadžmenta znanja: Wiiga[122], von Krogha i Roosa[118], Nonake i Takeuchija[46].

Wiigov model menadžmenta znanja[117] sledi princip: znanje mora biti organizovano, zavisno od svoje svrsishodnosti i korisnosti njega samog.[46] Sam Wiigov model smatra se daljom nadogradnjom i usavršavanjem modela Nonake i Takeučija, jer definiše različite nivoe internacionalizacije znanja. Wiigov model tvrdi na prvom nivou da internacionalizacija počinje sa ličnim znanjem i da sama osoba nije uopšte svesna znanja ili samo naslućuje kako to znanje može koristiti – „nivo novajlije". Drugi nivo je nivo „početnika" – lice koje je svesno postojanja znanja i odakle može da ga dobije, ali ne vidi razlog za to. Na trećem nivou su „kompetentne" osobe – osobe koje znaju da znanje postoji, koriste ga, uočavaju razlog njegovog postojanja, koriste baze znanja, dokumente i

pomoć drugih lica. Četvrti nivo je nivo „eksperta" – osoba koja zna da znanje postoji, memoriše ga, koristi sa razumevanjem i ugrađuje ga u vrednosti i sudove uz spremnost na posledice primene znanja. [117]

Wiigu svojim radovima [117][123][122][124] izdvaja tri forme znanja: javno znanje, zajedničko znanje i [illegible]o znanje. Javno znanje čini eksplicitno znanje dostupno u javnosti. Znanje koje je u vlasništvo radnika i koje se deli na njihovom poslu ili je ugrađeno u tehnologiju predstavlja zajedničko znanje odnosno iskustvo. Najpotpunije, ali i najteže znanje kome se pristupa je lično znanje. Wiig takođe, glavnim formama znanja dodaje još četiti tipa: faktičko, konceptualno, iščekujuće i metodološko...

U svom modelu organizacione epistemologije, Von Krogh i Roos prvi jasno razgraničavaju razliku između individualnog i socijalnog (društvenog) znanja.[118] Kroz epistemiološki pristup menadžmentu znanja oni odgovaraju na sledeća pitanja:

- Kako i zašto znanje dolazi do pojedinca u kompaniji?
- Kako kompanija i drugi društveni entiteti dolaze do njega?
- Šta je najvažnije za znanje pojedinca/kompaniju?
- Koje su prepreke menadžmentu znanja u kompaniji?[118]

U svom modelu menadžmenta znanja, Von Krogh i Roos zastupaju stav da je znanje locirano kako kod pojedinca, tako i u kompaniji, dok se na društvenom nivou stvara u odnosima između pojedinaca. [118] U smislu podsticanja i[illegible]vacija, dostignuća konkurentske prednosti i ostalih organizacijskih ciljeva izdvaj[illegible] se pet osnovnih činilaca koji utiču na uspeh ili neuspeh menadžmenta znanja: mentalni sklop pojedinca, komunikacija u kompaniji, organizaciona struktura, veze između članova i menadžment ljudskih resursa. [118]

U svojim teorijama menadžmenta znanja autori Nonaka i Takeuči zagovaraju spiralni model znanja koji se zasniva se na proučavanju korena uspešnosti japanskih kompanija.[46] Prema njihovim tvrdnjama japanske kompanije se okreću subjektivnom predviđanju i „tacit pristupu" menadžmenta znanja. Kreiranje znanja uvek počinje sa pojedincem. Ovako predloženi model treba da istakne dinamičnu prirodu procesa kreiranja znanja kako bi omogućilo efikasno upravljanje samim procesom menadžmenta znanja. Znanje koje akumulirano iz eksternog okruženja, deli se širom kompanije i koristi se u cilju razvoja novih tehnologija i proizvoda, čuva se u bazama znanja kompanije. Nonaka i Takeuči dolaze do tvrdnje da eksplicitno i tacitno „prećutno" (skriveno) znanje stvaraju novo znanje. Pri tome ističu da četiri procesa objašnjavaju stvaranje znanje: [46]

- socijalizacija – predstavlja proces razmene znanja između pojedinaca,
- eksternalizacija – predstavlja proces transformacije „prećutnog" znanja u eksplicitno, tj. pretvaranje ideja u konkretno znanje,
- kombinacija – predstavlja proces pretvaranja jednog eksplicirnog u drugo eksplicitno stanje i
- internalizacija – predstavlja proces u kome se eksplicitno znanje pretvara u „prećutno" znanje.

Kompanije i menadžeri u njima treba da budu orijentisani ka stvaranju eksplicitnog znanja, koje je po svojoj prirodi kolektivno. Ako se takvo znanje uvede u operacije kompanije, ono ne može nestati na kada pojedinac napustiti neku kompaniju. Neki izvori iz

literature ukazuju da se 10 – 20% eksplicitnih znanja kompanije nalaze u bazama podataka. [125]



Slika 12. *Proces kreiranja znanja*
Izvor: [114]

Kreiranje znanja zavisi od međusobne interakcije između prećutnog i eksplicitnog znanja koji se odvija kroz četiri navedenih modela a koja je pritom kontinuirana i dinamička. Sa slike 12 uočavamo da spirala znanja ukazuje kako kompanija prepoznaje, organizuje i sistematizuje individualno prećutno znanje. To je kontinuirana aktivnost toka znanja, deljenja i konv je znanja kako od strane pojedinca, tako i od strane kompanije u celini. Najteži koraci u spirali znanja su ona koja uključuju promenu u vrsti znanja. [114]

Model znanja Nonake i Takeučija smatra se najsnažnijim modelom u menadžmentu znanja. Prednost ovog modela je njegova jednostavnost i činjenica da polazi od dinamičke prirode znanja i procesa kreiranja znanja. Naravno, ovaj model ima i svoje nedostatke: nedovoljno objašnjenje svih faza, nedovoljno stavljanje akcenta na proces donošenja odluka u pogledu uravnoteženja između dve vrste znanja, kao i linearnost modela.

3.5 Implementacija menadžmenta znanja u praksi - Metode menadžmenta znanja

3.5.1 Brainstorming

Predstavlja grupnu tehniku za povećanje kreativnosti (sposobnosti generisanja i razvijanja novih ideja) u procesu poslovnog odlučivanja. Sastoji se u organizovanju grupnog sastanka, tokom kojeg se vrši prikupljanje mišljenja i stavova. Svaka ideja je dobrodošla, a od učesnika se traži puno mentalno učešće i kreativnost u okviru postavljenog zadatka. Osnovna pravila ove metode svode se u sledećem: poželjan je veći broj ideja kako bi se lakše dobila „ona prava"; ideje treba da se nadovezuju i poboljšavaju; sastanak prati dogovorenu agendu čak i kada „presuše ideje"; zapisuje se svaki odgovornema besmislenih ideja. Elementi procesa: iznalaženje ideja (svako izlaže svoju ideju); vrši se procena i izbor ideja (ideje se obrazlažu, povezuju, biraju najbolje); plan primene (šta, ko, kada). Nedostaci ove metode ogledaju se u ograničavanju produktivnosti, strahu od javnog istupanja i straha od ocenjivanja.

3.5.2 Učenje i prikupljanje ideja *(Learning and Idea Capture)*

Metod učenja i prikupljanje ideja (engl. *Learning and Idea Capture*) omogućava kolektivno i sistematično sakupljanje ideja i rezultata učenja u kompaniji. Ova metoda je korisna zbog težnje kompanija da budu kreativne, sakupe više ideja i usmere učenje ka boljem znanju koje će deliti, primeniti i istraživati. Nije problem u novim načinima učenja i idejama, već u njihovom efikasnom čuvanju. Kompanije koje ne sakupljaju ideje kako one nastaju, već samo s vremena na vreme, u zaostatku su u odnosu na kompanije koje to rade kontinuirano. Ova metoda se može koristiti upotrebom personalnih metoda, kao i kolektivnih metoda. Idealno je da se personalne metode inkorporiraju u kolektivne metode.

Nove ideje i rezultati učenja mogu biti sačuvani i u jednostavnom fomatu dokumenta koji treba da sadrži: datum i vreme, lice koja čuva ideju, situaciju, projekat ili posao, ime klijenta, lokaciju, kontekst, novu ideju ili učenje, sledeći korak.

3.5.3 Uključivanje znanja u projekat *(Peer Assists)*

Uključivanje znanja u projekat (engl. *Peer Assists*) kao metoda predstavlja ekonomičan i efikasan način za dizajn projekta i izbegavanje grešaka i propusta baziranih na iskustvu i znanju drugih. Ovo je metod razmene znanja i iskustva između dva tima ili dve poslovne jedinice u kompaniji, zasnovan na dijalogu i obostranom poštovanju. Metoda se primenjuje tako što tim započinje rad na novom projektu i poziva drugi tim sa iskustvom u oblasti za koju postoji interes u kompaniji. Radni tim tako dobija savete koji mogu biti osnova jednog novog pristupa a to je korišćenje već postojećeg znanja i iskustava. Trajanje ove metode je do dva dana. [126]

Prilikom učešća u ovoj metodi treba odrediti ograničenja. Broj učesnika je ograničen do šest jer je teško održati konstruktivnu diskusiju sa većim brojem učesnika. Potrebno je pozvati samo one članove time koji imaju iskustvo i potrebno znanje. Vođa projekta može primiti sugestije od članova tima u vezi sa potencijalnim učesnicima.

Sporovođenje ove metode vrši se u kroz sledeće korake:

- Nakon razjašnjavanja svrhe i ciljeva tim domaćin poziva tim sa iskustvom (6–8 članova).
- Određuje se vreme za socijalizaciju i stvaranje pozitivne klime među učesnicima.
- Prezenteri tima domaćina sažeto i precizno objašnjavaju projekat (10–15 min). Naglašavaju se specifične potrebe tima i očekivani rezultati.
- Tim posetilac objašnjava situaciju i svoje iskustvo.
- Tim posetilac identifikuje moguće opcije za rešavanje problema, tim domaćin pažljivo sluša i beleži sve opcije.
- Tim posetilac prezentuje finalni odgovor, tim domaćin mora da bude spreman da čuje i nešto što nije očekivao.
- Tim domaćin se obavezuje da će nastaviti sa ukazanim pravcem aktivnosti i redovno obaveštava drugi tim o tome.

3.5.4 Pregled naučenog *(Learning Reviews)*

Metodu pregled naučenog (engl. *Learning Reviews*) koristi projektni tim kako bi pomogao timskom i individualnom učenju tokom radnog procesa. Cilj ove metode je da članovi tima kontinuirano uče tokom realizacije projekta. Nije potrebno čekati da se završi

projekat, da se napravi pregled naučenog. Učenje tokom rada omogućava i pojedincima i timu da uče kako iz uspeha, tako i iz neuspeha, tokom trajanja projekta. Ova metoda sastoji se od dve faze: trenutno sprovođenje i imenovanje fasilitatora. Metoda predstavlja prostor za olakšavanje učenja, a ne platformu za kritiku. U primeni ove metode razlikujemo dva formata: format sastanka i format radionice (koji se više preporučuje).

Format sastanka odvija se kroz odgovorena sledeća pitanja: Šta je trebalo da se dogodi? Šta se zapravo dogodilo? Zašto je nastala razlika? Šta smo naučili? Kako bi se postiglo jednoglasno razumevanje cilja projekta ili same aktivnosti, diskusija počinje sa prvim pitanjem. Fasilitator treba da se fokusira na to kako se članovi tima ponašaju u vezi sa onim što se dogodilo, a ne samo na jednostavno prepričavanje događaja. Pravo učenje počinje kada članovi tima počnu da upoređuju plan sa onim što se stvarno dogodilo. Fasilitator je zadužen za pitanja članovima tima kako bi identifikovali jednu ključnu naučenu stvar koja može kasnije pomoći timu u budućnosti. Sve to potrebno je zabeležiti i sačuvati.

Format radionice realizuje se kroz upoznavanje sa dnevnim redom i označavanjem ključnih događaja i pitanja u projektu. Nakon toga vrši se kreiranje novog znanja, tako što se izvrši podela tima u manje grupe i zatraži od njih da nakon razmišljanja zapišu na samolepljive papiriće naučeno, nove ideje i pitanja. Tada se grupišu sva učenja i pitanja u prirodne klastere ili kategorije, a zatim izvrši diskusija i pregled. Predmet diskusije treba da budu ključni klasteri, a postavljaju se sledeća pitanja: Šta možemo uraditi bolje, sledeći put? Šta možemo zadržati kao benefit za sve buduće umove? Nakon toga rotiraju se grupe koje komentarišu i dodaju svoje komentare na zapažanja drugih grupa. Po završetku komentara vrši se konačna diskusija. Potrebno je dozvoliti članovima tima da zabeleže konačne zaključke i da se slože o budućim aktivnostima.

3.5.5 Naknadna ocena aktivnosti *(After Action Review)*

Metoda naknadna ocena aktivnosti (engl. *After Action Review*) predstavlja diskusiju o projektu ili aktivnostima nakon završetka projekta ili aktivnosti. Omogućava pojedincima koji su uključeni u projekat da iz sopstvenog iskustva nauče šta se dogodilo i zašto, šta je dobra strana svega što je realizovano, šta se može poboljšati i koje lekcije se iz datog iskustva mogu izvući. Podrazumeva otvorenost i usvajanje znanja, a ne rešavanje problema i utvrđivanje krivice. Obuhvata stvaranje dobre atmosfere pozivanjem kompetentnih ličnosti da učestvuju u aktivnosti. Najbolje optimalno vreme za primenu ove metode je od sastanaka dva pojedinca u trajanju od pet minuta do celodnevnog sastanka celog projektnog tima na kraju projekta. Važno je zabeležiti i podeliti najavažnije naučene lekcije.

Glavni razlog za korišćenje ove metode ogleda se u predstavljanju pregleda rezultata projekata nasuprot postavljenih ciljeva. Metoda može da čini osnovu za učenje iz projektnih uspeha ili neuspeha, i može da bude polazna tačka za unapređenje budućih projekata. Fokus ove metode je na učenju, a ne na krivici bilo kog člana u timu. Greške predstavljaju osnovu za učenje, a treba da se obezbedi atmosfera poverenja i otvorenosti. Moguće je i učešće spoljnih *stejkholdera*, a naučeno treba sačuvati u pisanoj formi ili u elektronskom formatu.

Nakon završetka projekta odmah se pristupa realizaciji ove metode. Potrebno je dati odgovor na sledećih pet pitanja: Šta je trebalo da se dogodi? Šta se zaista dogodilo? Šta je prošlo dobro i zašto? Šta je moguće unaprediti i kako? Koje lekcije se mogu koristiti u budućnosti? Važno je da se na početku izvrši razmatranje cilja i postigne saglasnost svih učesnika oko pravila diskusije. Fasilitator sledi sledeća uputstva u smislu: dozvoljeno

neslaganje; podsticanje članova da daju iskrena mišljenja; korišćenje otvorenih pitanja za vođenje diskusije i na kraju parafraziranje i sumiranje ključnih tačaka same diskusije.

3.5.6 Međusobno podučavanj *(Collegial Coashing)*

Međusobno podučavanje (engl. *Collegial Coaching*) predstavlja profesionalni metod čime se vrši unapređenje kolegijalnosti i poboljšanje rezultata. Zapravo predstavlja proces putem kojeg eksperti dele svoja iskustva jedan sa drugim, uz povratnu informaciju, podršku i pomoć u svrhu pregleda postojećih veština, učenja novih i/ili rešavanja problema.

Primenom ovog metoda ispunjavaju se sledeće funkcije:

- kolegijalnost (diskusija o uspesima i promašajima sa novim pristupom),
- povratna veza (uzajamni objektivan *feedback*),
- analiza (uzajamna pomoć za preuzimanje kontrole nad novim pristupom),
- adaptacija (zajednički rad na pristupu koji će odgovarati specijalnim zahtevima zadatka) i
- podrška (obezbediti potrebnu podršku).

3.5.7 Mentorstvo *(Mentoring)*

Mentorstvo (engl. *Mentoring*) predstavlja metodu prenosa znanja između generacija. Mentor je lice sa iskustvom koje je sposobno i raspoloženo da podučava lica sa manjim znanjima u određenoj oblasti. Osnovna svrha ove metode je unapređenje veština, generalno unapređenje kompanije i njene kulture kao i razvoj karijera zaposlenih u kompaniji. Preduslovi za sprovođenje ove metode su: određivanje ciljeva mentorstva, razvijanje dobrih odnosa između mentora i učenika i definisanje plana mentorstva.

Prilikom realizacije ove metode potrebno je slediti sledeće korake:

- određivanje ciljeva mentorstva,
- izabor pravog mentora,
- razvoj plana mentorstva,
- definisanje predmeta svakog sastanka i
- na kraju razdvajanje od mentora (kada učenik postane dovoljno jak).

3.5.8 Sistem najbolje prakse *(Good practice)*

Sistem najbolje prakse (engl. *Good practice*) kao metoda daje pokazatelje da nešto što je bilo efikasno u jednom slučaju, može to isto biti i u nekom drugom. Ovom metodom sprečava se gubitak vremena i novca. Osnovni cilj ove metode je omogućavanje pronalaska i korišćenja nečeg što već postoji. Ovom metodom ljudi dobijaju znanje koje im je potrebno i koje im omogućava stvaranje odgovarajućeg i kompletnog konteksta za njih.

Sistem najbolje prakse predstavlja najčešće primenjivanu metodu menadžmenta znanja. Najčešće počinje u kompanijama u vidu instrukcija i uputstava. Zasniva se na učenju od drugih i ponovnom korišćenju znanja koje poseduje. Prednost ove metode je dobro razvijen proces baziran na akumuliranom iskustvu i znanju kompanije. Najčešće predstavlja kombinaciju dva elementa:

- eksplicitnog znanja – baza podataka dobre prakse (povezuje ljude i informacije)

i

- metoda za razmenu znanja – zajednica prakse (međusobno povezuje ljude).

Najdelotvorniji način primene je način *on the job*, gde se vrši povezivanje zajednica i lični kontakt sa ostalima koji koriste dobru praksu u kompaniji.

Podrazumeva sledeće korake:

- identifikacija zahteva korisnika,
- identifikacija dobre prakse koja je vredna deljenja,
- dokumentovanje dobre prakse,
- potvrda dobre prakse sa postignutim rezultatima u novom kontekstu,
- širenje i primena dobre prakse i
- razvoj odgovarajuće infrastrukture podrške.

3.5.9 Izlazni intervju *(Exit Interview)*

Izlazni intervju (engl. *Exit Interview*) predstavlja metodu da se znanje zaposlenih koji napuštaju kompaniju zadrži unutar nje. Predstavlja način i da se definiše znanje o tome šta je sve neophodno kako bi se određeni posao u kompaniji realizovao. Ovaj intervju može biti *win – win* situacija i za kompaniju i za bivšeg zaposlenog, ako se realizuje u potpunosti. Na taj način, kompanija zadržava znanje zaposlenog koji odlazi, čini ga dostupnim ostalima, dok pritom bivši zaposleni na jedinstven način definiše svoj jedinstveni doprinos kompaniji i ostavlja neki „svoj pečat". Metoda je relativno brza i nije skupa. Preporučena forma ovakvog intervjua je „licem u lice".

U realizaciji ove metode potrebno je slediti sledeće korake:

- Potrebno je početi na vreme. Planirati potencijalne odlaske i eventualne njihove zamene drugim zaposlenim.
- Identifikacija lica koji bi mogli imati benefite od zadržanog znanja i provera njihovih interesa.
- Izbor lica koja će realizovati intervju.
- Dokazati da je eksplicitno znanje bivšeg zaposlenog dostupno.
- Utvrđivanje ključnih pitanja za tacitno znanje lica koje odlazi iz kompanije.
- Pronalazak načina identifikacije uspešne priče i faktora uspeha, problema i potencijalnih opasnosti.
- Utvrđivanje izvora znanja (lica, mreže...).

3.5.10 Pričanje priča *(Storytelling)*

Pričanje priča (engl. *Storytelling*) predstavlja inspirativno sredstvo komunikacije za deljenje znanja. Način na koji se koristi je iskustveno orijentisan i autentičan, dok je forma narativna i većina ljudi je smatra interesantnom i atraktivnom. Ova metoda se koristi kada postoji jasna orijentacija na informacione tehnologije u kompaniji. Predviđen je i vodič za onoga ko priča priču.

- Potrebna je jasnost u vezi sa porukom koja se želi preneti pričom.

- Izgradnja priče na sopstvenom iskustvu.
- Početi priču od početka. Izgraditi atmosferuznatiželje. Ispričati momenat iznenađenja dramatičnim glasom. Posmatrati svoje slušaoce.
- Povezati priču sa temom o kojoj se diskutuje u kompaniji.

A isto tako predviđen je vodič i za one koji slušaju priču:

- Potrebno je dati doprinos dobroj klimi u grupi. Pokazati interesovanje. Dati pripovedaču adekvatan razlog za priču.
- Potrebno je imati motivisanu publiku koja pažljivo sluša, razume i sarađuje.
- Nedostatak otpora priči. Odslušati pa tek onda postaviti odgovarajuća pitanja.
- Uspostavljanje atmosfere poverenja. Prekršiti je samo ako se primeti da pripovedač ne govori istinu.

U korišćenju ove metode predviđeno je pet koraka.

- Identifikacija ključnih oblasti znanja koje se žele preneti i podeliti u kompaniji.
- Izabrati lica sa bogatim znanjem i iskustvom i angažovati ih da ispričaju priču.
- Objava održavanja sesije.
- Održavanje sesije.
- Ocenjivanje rezultata.

Preporuka je da se sastanak snimi i pošalje zaposlenima. Poželjno je formiranje zajednice prema temama između učesnika koji imaju jak interes za učešće. Potrebno je obezbediti uslove kako bi održavanje sesije bilo regularno i redovno. Time bi se omogućilo svim zaposlenima mogućnost da ispričaju priču.

3.5.11 Kafe znanja *(Knowledge Cafe)*

Primena metode kafe znanja (engl. *Knowledge Cafe*) predstavlja način organizovanja grupne diskusije, kako bi se razmislilo, a nakon toga razvile i podelila mišljenja, na nekonfrontirajući način. Ova metoda za razliku od uobičajenih načina vodi do dubljih razmišljanja i deljenja znanja u kompaniji.

Kako bi metoda bila efiksna zahteva određen proces koji je potrebno realizovati. Ovu metodu trebalo bi koristiti na sledeći način. Kada je završena uvodna sednica, grupa se deli na male grupe, sa oko pet lica u svakoj grupi. Svaka grupa razmatra pitanja do 45 minuta. Male grupne diskusije ne vodi fasilitator. Učesnici se zatim vraćaju u krug, a fasilitator vodi grupu kroz finalnu sesiju u trajanju od 45 minuta, u kojoj učesnici, na osnovu malih grupnih diskusija, dele razmišljanja i ideje koje će se pojaviti tokom diskusije.

Pravila za sprovođenje ove metode su:

- Najveća efikasnost – između 15 i 50 učesnika.
- Idealan broj učesnika do 30.
- Optimalno trajanje: 1–2 sata.
- Jedino čvrsto pravilo: najveći deo vremena razgovor i diskusija.
- Prezentacije i druga povratna obrazloženja su nepoželjna.

Razlog zašto koristiti ovaj metod leži u tome da se danas u kompanijama zaposlenima često ne daje prilika da učestvuju u razgovorima i diskusijama. Zaposleni su obično pod pritiskom performansi kompanije. Periodična primena ove metode pruža mogućnost zaposlenima da razgovaraju, a oni sa ovih sesija odlaze više motivisani i inspirisani za rad u kompaniji.

3.5.12 Zajednica prakse *(Community of Practice)*

Metodu zajednice prakse (engl. *Community of Practice*) možemo posmatrati kao mrežu ljudi koji imaju zajednički interes ili problem u specifičnoj sferi kompetencija i spremni su na zajednički rad tokom određenog vremena i na učenje, razvijanje i deljenje znanja u svrhu doprinosa boljem radu kompanije. Ovakve zajednice formiraju se namerno ili spontano kako bi se delile ili kreirale zajedničke veštine, znanja i iskustvo između zaposlenih u kompaniji. Omogućavaju deljenje zajedničkog znanja između organizacijskih celina u kompaniji, ruše se barijere u protoku znanja kroz kompaniju. U ovoj metodi mogu da učestvuju od dva do tri lica do nekoliko hiljada ljudi, homogenog ili heterogenog sastava eksperata kompanije. Cilj ove metode je prevashodno povezivanje. Ovakve zajednice traju onoliko koliko to žele članovi zajednice.

Životni ciklus zajednica prakse realizuje se kroz planiranje, početak, rast, održavanje i prestanak rada zajednice. Najvažniji član zajednica prakse je koordinator zajednice. On ima dva zadatka: da pomaže zajednici da razvije praksu i da pomaže zajednici da se razvija kao zajednica. Karakteristike zajednica prakse su:

- jaka zajednica,
- jasno i dobro definisan domen,
- povezanost sa sopstvenom praksom,
- lična motivacija i
- neformalna struktura.

U sprovođenju ove metode razlikujemo četiri koraka:

- Potrebno je pronalaženje mogućnosti za povezivanje ljudi u neophodnim potrebama kompanije. Pronaći takve mogućnosti za povezivanje ljudi i podelu znanja koja može da stvori razliku u praksi kompanije.
- Uputiti poziv kompetentnim ljudima. Razgovor o dizajnu zajednice sa njima treba da odgovori na sledeća pitanja:
  - Šta je strateški kontekst zajednice?
  - Koje je ključno znanje koje će se deliti i kreirati?
  - Ko su potencijalni učesnici koji imaju koristi i mogu doprineti zajednici?
  - Koje su ključne aktivnosti koje podržava zajednica?
  - Gde mogu članovi zajednice da ostvare (fizičku i virtuelnu) interakciju?
  - Koje su ključne vrednosti i za organizaciju i za učesnike?
- Pokretanje zajednice druženjima.
- Napraviti rezultate kroz aktivnosti i deliti priče.

Kod primene zajednice prakse osnovna su četiri pravila:

- Obezbediti da su ključni *stejkholderi* kompanije članovi.
- Boriti se za praktične i vidljive rezultate koje treba objaviti i širiti.
- Pažljivo odrediti način povezivanja.
- Kombinovati neformalnost sa osnovnim pravilima komunikacije i saradnje.

Samo funkcionisanje zajednice prakse pokazuje nam i neke ključne podsticaje. Pojavljuju se *stjuarti* znanja: ključna lica koja su eksperti za određenu oblast i spremna su da preuzmu brigu za zajednicu prakse, i najvažnija su komponenta svake zajednice praksi. Za funkcionisanje ove metode u principu nisu potrebni veštački podsticaji kao što su novac ili promocija. Veoma je važno da zajednica odgovori na probleme za kojima učesnici tragaju, da mogućnosti rasta i razvoja ili samo bude intelektualna zabava na određenu temu.

Sprovođenje ove metode zahteva određene fizičke/virtuelne prostore, kao i društvene forme koje zahtevaju prostor u kome učesnici mogu da komuniciraju. Ako zadovoljava potrebe učesnika to može biti čak i virtuelni prostor. Zajednica prakse može da zahteva i upotrebu informacione tehnologije. Neke zajednice ne zahtevaju bilo koju IT, dok je to ključna platforma za razmenu znanja i ključne aktivnosti za druge zajednice.

Ovde je potrebno napomenuti da je za primenu ove metode potrebna podrška rukovodstva kompanije. Podrška rukovodstva – menadžmenta kompanije omogućava učesnicima ne samo da shvate značaj aktivnosti zajednice prakse, već i obezbeđuje potrebne resurse. Takođe, podrška rukovodstva može da utiče i na spontani karakter zajednice prakse.

3.5.13 Sajam znanja (Knowledge Fair)

Sajam znanja (engl. *Knowledge Fair*) kao metoda predstavlja događaj kreiran da prikaže informacije o kompaniji ili aktuelnoj temi u kompaniji. Osnovne karakteristike ove metode su:

- Predavanja, prezentacije, radionice, izložbe.
- Dostupnost informacija.
- Direktna komunikacija sa prezenterom.

Posetioci se kasnije često međusobno umrežavaju. Ova metoda je pogodna za primenu u situaciji kada imamo veliku količinu informacija za deljenje i gde je većem broju posetilaca potrebna šira perspektiva.

Koraci u sprovođenju ove metode:

- Objavljivanje informacije o sajmu.
- Organizovanje sajma tamo gde ima puno prostora na vidnom mestu.
- Realnost u određivanju vremena za prezentaciju.
- Ne suviše detaljno planiranje.
- Ne treba biti suviše ozbiljan – sajam znanja može i treba da bude zabavan!

3.5.14 Žute strane *(Yellow Pages)*

Primena metode žutih strana (engl. *Yellow Pages*) pomaže zaposlenima da pronađu druge zaposlene u kompaniji (ili van nje) koji poseduju adekvatno znanje i veštine

potrebne za određeni zadatak ili projekat. Osnovne karakteristike ove metode su da se u smislu prikaza preporučuje kao elektronski oblik, da pomaže kompaniji „da zna šta zna", da pronalazi ljude i omogućava pristup njihovom skrivenom, prećutnom znanju koje poseduju.

Koraci u primeni ove metode:

- Odrediti jasan cilj: Koji je cilj *Yellow Pages* u vašoj kompaniji?
- Kreirati odnos sa ljudima koji doprinose sistemu ili koriste sistem.
- Napraviti balans formalnih ili neformalnih informacija u kompaniji.
- Organizovati jednostavne ulaske.
- Redovno ažuriranje.
- Ohrabriti korišćenje žutih strana u kompaniji.

Ključevi uspeha ove metode leže u dobrovoljnom učešću, dovoljnom broju ljudi u bazi podataka kako bi ona bila validna i privukla na korišćenje, omogućavanje olakšanog korišćenja (ček liste ili padajuće liste, jednostavna objašnjenja i uputstva) i neophodne konsultacije sa ekspertima. Veoma je važna neophodnost stalnog ažuriranja podataka.

3.5.15 Posebne vrste baze znanja *(Wikis)*

Posebne vrste baze znanja metoda Viki (engl. *Wikis*) takođe se mogu koristiti u kompanijama. Obično je potrebno da baza sadrži stranicu za svaku temu. Teži da bude otvorena za mnoge koji mogu da da sarađuju, razvijaju i pristupaju novim znanjima u kompaniji. Viki spada u nestrukturisane baze znanja što znači da je moguće slobodno i poželjno dodavanje tema u bazi. Primena Viki metode može se vrlo brzo proširiti kroz kompaniju.

Korišćenjem ove metode sprečava se situacija da deljenje znanja u kompaniji zavisi od produktivnosti nekoliko ljudi. Kroz ovu metodu omogućava se mnogo većem broju ljudi u kompaniji da kreiraju, razvijaju i pristupaju novom znanju, kao učesnici, daju povratne informacije, pa i da stvaraju novo znanje tamo gde je potrebno. Baze znanja kao što je Viki daju pun kontekst strukturiranjem pitanja „šta, zašto, ko, gde, kada i kako"? Ovakvu bazu mogu stvoriti sami korisnici, dok je podrška IT sektora dobrodošla.

Realizacija metode Viki vrši se u četiri koraka.

- Utvrđivanje ključne oblasti znanja kojom se želi bolje upravljati.
- Odluka da li je potrebno otvoriti bazu znanja ili upravljati njom.
- Imenovati menadžera baze znanja.
- Napraviti bazu znanja.

3.5.16 Blog

Blog kao metoda predstavlja vrlo jednostavan sajt u stilu časopisa koji sadrži listu unosa, obično u obrnuto hronološkom redosledu. Unosi (postovi) su obično kratke priče ili članci, koji se često odnose na tekuće događaje, a mogu biti i fotografije, video-snimci ili audio-snimci. Sadržaj bloga može biti kreiran od strane jednog autora ili više njih. Osnovne karakteristike bloga ogledaju se u tome da je sadržaj bloga u suštini linearan. Blog ima fokus i ima mehanizam kroz koji čitaoci – posetioci mogu da komentarišu stavke. Blog poseduje elektronski indeks koji omogućava ljudima da automatski budu

obavešteni kada je nešto novo dodato u sadržaju.

Prednosti bloga ogledaju se u tome što softver koji se koristi, jednostavan je za korišćenje. Proces unosa postova na blogu je jedan od najlakših načina angažovanja u deljenju znanja. Jednostavnost bloga, zajedno sa sposobnošću za čitaoce da se automatski obaveštavaju o novim unosima, čini proces distribucije znanja vrlo jednostavnim. Blogovi nude jednostavan način za pojedince, timove i čitave kompanije da prikupljaju i objavljuju informacije o konkretnim temama i da ove informacije učine dostupnim, automatski, željeno širokoj publici.

Pravila za korišćenje bloga:

- Odlučiti u koju svrhu se piše i koji ton treba da bude preovlađujući na blogu.
- Odrediti teme koje će blog pokriti.
- Složiti se oko toga ko će pisati unose na blogu.
- Odlučiti kako promovisati blog.
- Kreirati blog – ako ste u većoj kompaniji, konsultujte se sa IT odeljenjem.
- Napraviti prvi post.
- Nastavitisa aktivnostima – suština blogova je u stvaranju korisnih sadržaja.

Blog je koristan i odgovarajući alat za komunikaciju sa širom publikom. Realna vrednost blogova leži u sposobnosti kreiranja jednostavnih načina za komuniciranje novih i zanimljivih informacija. Vremnom, sadržaj bloga može da postane veoma korisna, vredna za pretraživanje baza znanja. Blog ne treba koristiti za informacije koje se često revidiraju.

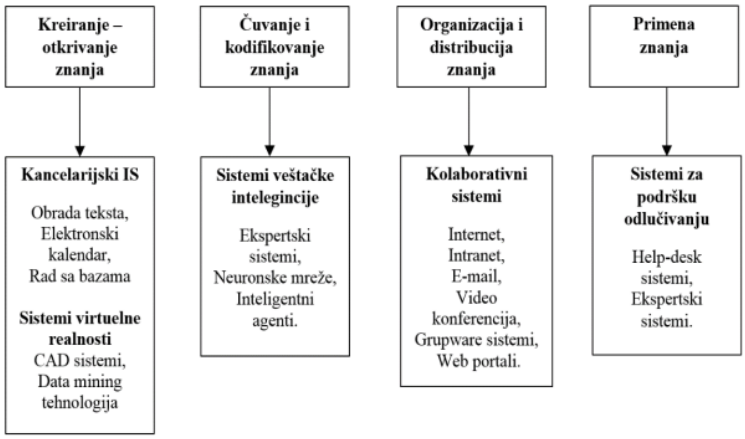
3.6 Tehnologije i alati za menadžment znanja

Poslovni sistemi teže da postignu svoje ciljeve primenom koncepta menadžmenta znanja u praksi. Razlozi za primenu sistema za menadžment znanja mogu se rangirati procentualno prema najvažnijim benefitima: [127]

- povećanje uspešnosti i prihoda (67%);
- zaštititi talenata i stručnosti (54%);
- unapređenju usluga i zadovoljstva korisnika (52%);
- učešću na tržištu u borbi sa konkurencijom (44%);
- kraćem vremenu stvaranja novih proizvoda (39%);
- ulasku u nove tržišne segmente (39%);
- smanjenju troškova (38%).

Između 50% i 95% znanja se prenosi usmenom i direktnom komunikacijom. Tako se izgubi veći deo znanja, pa uglavnom kompanije upotrebljavaju oko 20% organizacionog znanja. Tehnološku osnovu koja pomaže upravljanju znanjem u poslovnim sistemima čini sistem menadžment znanja (engl. *Knowledge Management Systems, KMS*). Ovi sistemi se zasnivaju na primeni savremenih tehnologija, a odabir tehnologije, alata i metoda predstavlja ključan korak za implementaciju strategije menadžmenta znanja u poslovnom sistemu (slika 13). Uspešna implementacija sistema menadžmenta znanja uslovljena je posedovanjem informacija o infrastrukturi neophodnoj za kreiranje i skladištenje znanja

kao i povećanje brzine stvaranja i prenosa znanja putem informacionih tehnologija. [5] Sistem menadžmenta znanja podržan je informacionim i komunikacionim tehnologijama koje kombinuju i integrišu funkcije za kontekstualizaciju kroz kompaniju i eksplicitnog i tacitnog znanja. Osnovna namena ovog sistema je da se znanje iz prošlosti implementira u sadašnje aktivnosti u cilju povećanja efikasnosti poslovnog sistema, dok krajnji cilj predstavlja podrška dinamičnom učenju kompanije i njenom efikasnom funkcionisanju. [128]



Slika 13. *Klasifikacija sistema za menadžment znanja*
Izvor: [114]

Postoji širok spektar tehnologija i alata za menadžment znanja. Pre izbora alata koji će se integrisati u sistem menadžmenta znanja poslovnog sistema, najpre je neophodno sagledati njihovu namenu i mogućnosti. Za tu namenu pogodno je primeniti metodologiju procene alata prema sledećim karakteristikama tipa alata (za stvaranje, organizaciju i podelu znanja) [129]:

- namena alata (opšta ili specifična),
- tip alata – za stvaranje, organizaciju i podelu znanja,
- vrsta znanja (strukturirano, nestrukturirano),
- oblik znanja (tekst, brojevi, grafika, audio/video zapis, slike) i
- metode koje alat koristi za menadžment znanja – u zavisnosti od tipa alata.

U nastavku će ukratko biti opisani sistemi za menadžment znanja koji su klasifikovani na osnovu realizacije procesa (slika 13): [114]

– Sistemi za automatizaciju kancelarijskog poslovanja u formi skladišta eksplicitnog znanja kao i sistemi za upravljanje dokumentima omogućavaju. [5]

– Sistemi veštačke inteligencije (engl. *artificial intelligence, AI*) u formi izučavanja mehanizama inteligentnog ponašanja kroz projektovanje, razvoj i procenu veštačkih tvorevina u koje ugrađuju ti inteligentni mehanizmi. Primeri inteligentnih sisteme spadaju: ekspertni sistemi[130], veštačke neuronske mreže, *Web* inteligentni agenti [131], tehnologije za kolaboraciju i komunikaciju, sistemi za obradu prirodnog jezika, sistemi za prepoznavanje govora i dr.

Prikupljanje poslovnih podataka, njihovo objedinjavanje na jednom mestu i analiziranje predstavlja zadatak poslovne inteligencije. Poslovna inteligencija obuhvata

metodologije, tehnologije i platforme za skladištenje podataka (engl. *Data Warehouse, DW*), OLAP procesiranje podataka (engl. *Online Analytical Processing, OLAP*) i rudarenje podataka (engl. *Data Mining*). Alati poslovne inteligencije (engl. *Business Intelligence – BI*) omogućavaju: pristup podacima iz jednog ili više različitih izvora, pregled podataka, analizu podataka i distribuciju znanja dobijenog analizama. [132]

Skladišta podataka (engl. *Data Warehouse – DW*) kao analitičke baze podataka predstavljaju osnovu sistema za podršku odlučivanju, sa osnovnom namenom da odražava procese i pravila poslovanja kompanije u celini. Ona vrše prečišćavanje i agregaciju podataka iz radnih sistema i smeštaju u dimenzionalne baze podataka. Ovako organizovani podaci pomažu u ocenjivanju stanja poslovnih situacija, trendova, projekcija i alternativa u svrhe podrške odlučivanju.[132] OLAP alati za upite i izveštaje (engl. *Online Analytical Processing, OLAP*) – predstavljaju moćan multidimenzionalni alat koji omogućava veoma brze odgovore na postavljane upite. Alati za rudarenje podataka (engl. *Data Mining*) pronalaze trendove u podacima koji se ne mogu identifikovati prostim analizama. U suštini, termin *Data Mining* označava dva naučna pojma: otkrivanje i predviđanje.

Efektivniji sistem za menadžment znanja u kompanijama realizuje se primenom novih tehnologije i razvijanjem odgovarajuće ICT infrastrukture, koja stvara uslove za efikasno odlučivanje u kompaniji. Kao i za svaki drugi projekt i novi sistem, tako se i za sistem menadžmenta znanja postavlja pitanje ključnih koristi za kompaniju i za njene zaposlene.

Ključne koristi za kompaniju ogledaju se u podsticanju kreativnosti, timskog rada i istraživačkog pristupa poslovanju, kvalitetnijem korišćenju postojećeg znanja u okviru kompanije, učenju iz iskustva, efikasnijem korišćenju zajedničke baze znanja, povezivanju eksperata, samostalnom razvijanju novog znanja, poboljšanju procesa za upravljanje dokumentacijom, stvaranjem projektne dokumentacije, kao i povećanje kvaliteta proizvoda, i zadovoljstva korisnika kvalitetom proizvoda i usluga.[132]

Ključni benefiti za zaposlene ogledaju se kroz identifikaciju eksperata u radnom okruženju, mogućnostima za profesionalni razvoj organizovanjem obuka, kvalitetnije izvođenje poslovnih zadataka na radnom mestu, razvoju lične mreže eksperata, stvaranja fleksibilnog i dinamičnog radnog okruženja, povezivanje lica sa sličnim interesima, brže rešavanje problema i povećanje zadovoljstva i motivacije zaposlenih.[132]

3.7 Perspektive koncepta menadžmenta znanja

Menadžment znanja je važan zadatak u svakoj kompaniji i svaka pojedinačna poslovna jedinica treba da stvara i prikuplja znanje koje je potrebno na operativnom nivou kompanije. Odgovornost korporativnog centra je u tome da razjasni koje je tačno znanje od strateške važnosti za kompaniju. Samim tim, zadatak korporativnog centra je da stvara okolnosti u kojima će znanje biti kreirano i da određuje koje je to znanje koje povećava vrednost kompanije.

Važno je znati šta želimo da znamo. To je prvi korak koji bi trebalo preduzeti kako bi smo bili sigurni da je znanje koje prikupljamo potrebno znanje. Korisno oruđe koje može pomoći u tome je mapa znanja koja pokazuje koje su oblasti kritične za budućnost kompanije. Ona deli znanje na manje jedinice, koje se ponašaju kao linkovi između pojedinih segmenata znanja. Prvi korak u projektovanju mape znanja je projekcija poslovne strategije kompanije u ključnim oblastima znanja. Nakon toga se uspostavljaju

linkovi znanja koji povezuju i jačaju srodno znanje tako da omogućavaju iskorišćavanje njihove sinergije. Zatim definišu se segmenti znanja kao celokupno znanje koje radnici znanja i sistemi znaju o određenoj temi povezanoj sa ostvarenjem poslovne strategije.

Dobra mapa znanja je važno oruđe za upravljanje tokovima znanja. Može pomoći u definisanju strategije i usmeravanju kreiranje znanja; kako bi se ustanovilo gde naše inicijative za upravljanje tokovima znanja imaju najveći uticaj na dodatnu vrednost. Dobija se savršeni šematski plan za intranet koji može da prikaže kako organizovati znanje u centre kompetentnosti ili centre za perfekciju. Može da se kombinuje sa „mapom izvora" koja sadrži i izvore znanja u okviru određenih segmenata znanja. Može biti važno oruđe za bolje upravljanje kompetencijama radnika znanja.

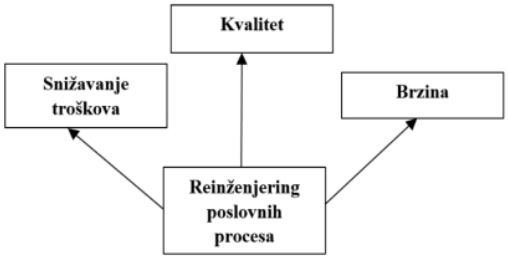
4. Konceptualna tehnološka infrastruktura

Postojanje moderne fleksibilne kompanije koja se prilagođava zahtevima promena u svojoj okolini i pravovremeno reaguje na njih, preduslov je koji traži nova ekonomija zasnovana na znanju. Samo one kompanije koje su svoju strukturu formirale tako da mogu da se prilagođavaju promenama, da se razvijaju, menjaju i uče, da kontinuirano kreiraju proizvode ili usluge, mogu biti sigurne u svoj opstanak. Pod tim pristupom podrazumeva se postojanje napredne tehnološke infrastrukture u kompaniji. Pre svega potrebno je postojanje stalne procene sopstvenog poslovanja i spremnost na reorganizaciju kako poslovanja, tako i reinženjeringa poslovnih procesa u kompaniji. Te promene moraju biti usklađene sa stvarnim potrebama kompanije i tržišta, na temelju opravdanih razloga i trebaju biti usmerene na tehnološko praćenje trendova i budućnosti. Potrebno je imati u vidu i činjenicu da često restrukturiranje i sprovođenje reinženjeringa poslovnih procesa može izazvati i negativne posledice i ugroziti već stečenu poziciju kompanije na tržištu te treba biti oprezan u tom smislu.

4.1 Reinženjering

Reinženjering predstavlja pristup, kojim se omogućavaju radikalna poboljšanja, menja stav zaposlenih kada su u pitanju performanse procesa, stvaraju izazovi za drugačije sagledavanje procesa i razmišljanje o performansama. Rezultat reinženjeringa treba da bude nova strateška vizija, koja postaje mnogo važnija od same tehnologije u kompaniji.[133] Sva dešavanja u svetskoj ekonomiji naterala su savremene kompanije da preispitaju dosadašnje načine delovanja i preduzmu radikalne promene u dosadašnjem poslovanju. Ovakvi zahtevi i promene vrše pritisak na kompanije da stalno redefinišu i redizajniraju već standardne procese kako bi poboljšali svoje poslovanje. Uvođenje novih grupa ideja, novih postupaka i načela obuhvaćeno je pojmom reinženjering poslovnog procesa.

Sama suština reinžinjeringa nije izvršiti modifikaciju postojećih poslovnih procesa, manjim ili parcijalnim zahvatima, već da se sveobuhvatnim redefinisanjem postojećih poslovnih procesa kompanije postignu unapređenja ključnih parametara poslovanja kao što su troškovi, kvalitet i brzina (slika 14).[134] Reinženjering se obično fokusira na nekoliko ključnih poslovnih procesa kompanije koji su bitni za njen uspeh unutar sektora na tržištu u kome ona posluje.



Slika 14. *Ključni parametri na koje se fokusira reinženjering*
Izvor: [134]

Pod reinženjeringom se podrazumeva započinjanje određenih procesa u kompaniji iz početka sa akcentom na: [98]

- temeljnost,
- korenitost,
- drastičnost i
- usmerenost na procese.

Suština reinženjeringa ogleda se u promeni načina poslovanja. Umesto standardnih postupaka, reinženjeringom se osmišljavaju i ugrađuju inovativna rešenja koja zahtevaju novi pristup i u celini obuhvataju ključne procese u kompaniji. Realizacija reinženjeringa u kompaniji podrazumeva novi pristup prema radu i uvođenju promena koje bi trebalo da rezultiraju: [135]

- ukidanje mnogih nivoa nepotrebnih koordinacija i kreiranje jednostavne hijerarhijske organizacione strukture kompanije,
- formiranje ekipa procesa umesto funkcionalnih odseka,
- uska specijalistička obuka zamenjuje se opštim obrazovanjem,
- specijaliste zamenjuju generalisti sposobni da izvrše multidimenzionalne zadatke,
- menadžeri postaju treneri umesto strogih kontrolora, a pojedinci se osamostaljuju i postaju ovlašćeni nosioci poslova sa većom autonomijom,
- napredovanje se sprovodi na osnovu sposobnosti pojedinca,
- nagrađivanje i merenje rada meri se uspešnošću proizvoda ili usluge na tržištu,
- prelazi se na rad usmeren ka korisniku.

Samo izvođenje reinženjeringa poslovnog procesa karakterišu tri faze: otkrivanje, redizajn i realizacija. [134] Faza otkrivanja je ključna u ispitivanju poslovanja radi pronalaženja mogućnosti i ključnih procesa nad kojima će se sprovesti reinženjering. U drugoj fazi implementira se redizajn odabranih procesa tokom kojeg se definišu detaljni planovi izvođenja postupaka reinženjeringa. Treća faza označava fazu realizacije i implementacije rešenja u kompaniji. [134]

Postoje različiti motivi zbog čega se kompanije odlučuju za reinženjering. Liderske kompanije se odlučuju na to kako bi još više učvrstile svoje liderske pozicije, dok druge kompanije to rade kako bi dostigle konkurenciju. Jedan od razloga može biti i uvođenje novih tehnologija, informaciono-komunikacionih tehnologija, što dovodi do automatizuje i ubrzavanja procesa. Suprotno od toga, neke kompanije se odlučuju na reinženjering tek kad su pred kolapsom. Tada su poslovni procesi zastareli i nerentabilni i ovakve kompanije su pred zatvaranjem i nestaju sa tržišta. One su tada prinuđene da vrše primenu novih poslovnih strategija koje podrazumevaju drastične promene, odnosno zahvate koji su karakteristični za reinženjering.

4.2 Uvođenje savremene organizacione strukture u kompaniji

Svaka kompanija koja je pripremljena da reaguje na promene u svom okruženju, mora neprekidno da preispituje svoju unutrašnju snagu i slabosti. To čini kroz preispitivanje svoje postojeće organizacione strukture i svoje prilagodljivosti promenama, naročito u situaciji ako je sama kompanija odlučila da izvede redizajn svog poslovanja. Analizom raznih primera iz prakse može se zaključiti da se formiranje organizacionih

jedinica vrši prema funkcionalnom principu kompanije.

4.2.1 Funkcionalna organizaciona struktura

Predstavlja najstariji i najrasprostranjeniji organizacioni oblik u kompanijama. Ovakav funkcionalni oblik predstavlja grupisanje istorodnih, sličnih ili direktno zavisnih i uslovljenih poslova, tako da se poslovi date funkcije međusobno povežu i svrstaju u odgovarajuću organizacionu jedinicu – sektor [136]. Grupisanje i povezivanje poslova direktno je povezano sa formiranjem organizacionih jedinica kompanije prema poslovnim funkcijama.[137] Grupisanje po funkciji predstavlja istovremeno i grupisanje prema sličnim profesionalnim sposobnostima. Ovakvim funkcionalnim grupisanjem kombinuju se slične aktivnosti i zadaci, jer su oni često međuzavisni i potrebno je da se vrši njihova koordinacija.

Ovaj oblik organizacione strukture karakterističan je za kompanije koje u svom poslovanju žele da implementiraju prednosti ekonomije obima.[137] Prednost organizovanja po fukcionalnom principu je u njenoj jednostavnosti, koja proizilazi iz važne karakterirstike ovog kriterijuma – sličnost aktivnosti. Stručnost, efikasnost i kreiranje obima karakteriše rad u funkcionalnim celinama. Takođe, prisutan je visoki stepen specifičnosti pojedinih poslova, primena jednoobraznih metoda i tehnika, racionalna upotreba prostora i opreme, stručno vođenje i jedinstvena koordinacija.

Ograničenja ovakvog načina organizacije ogleda se u preteranoj centralizaciji autoriteta zbog potrebe za koordinacijom. Funkcionalno uređenje stvara međuzavisnost jer celokupan posao ne može da se obavi bez saradnje svakog dela kompanije. Kao posledica toga, nivo odlučivanja se stalno pomera naviše, tako da se može izvršiti koordinacija aktivnosti organizacionih celina. Isto tako menadžeri tih organizacionih celina koji su specijalisti za svoju profesiju, teže ka tome da razmišljaju u terminima sopstvene specijalnosti i da donose odluke ne uzimajući u obzir povezanost njihovih aktivnosti sa ostatkom kompanije. Loše strane se ispoljavaju i u sporom prilagođavanju promenama u poslu i okolini, nedostatku saradnje i timskog rada, što su predstavlja elemente koji presudno utiču na sposobnost razvoja i opstanka kompanija u današnjim uslovima tržišnog poslovanja.

4.2.2 Procesna organizaciona struktura

Na kompanije se vrši pritisak da na najproduktivniji način iskoriste raspoloživi ljudski potencijal. Striktna podela radnih zadataka u okviru funkcionalnih jedinica ne može da odgovori na sve zahteve, naročito u situacijama kada se javi potreba za forimaranje tima čiji sastav čine lica iz različitih funkcionalnih jedinica kompanije.

Procesna organizaciona struktura najčešće se javlja kao kriterijum za dodatnu organizacionu strukturu zbog ekonomičnijeg načina oblikovanja poslovnih procesa. Bazirana je na radnim odnosno poslovnim procesima kao glavnim kriterijumima za formiranje organizacionih jedinica i radnih timova, umesto na poslovnim metodama. [137] Skraćuje vreme potrebno za izvršenje poslova i zahteva procesne timove, koji se formiraju iz pojedinih poslovnih funkcija koju trebaju da izvršavaju određene poslove u procesu. Svojom orijentacijom uklanja slabosti i rigidnosti funkcionalne organizacione strukture tako da okupi ljude iz specifičnih poslovnih funkcija u procesne timove koji izvršavaju određene zadatke u konkretnom poslovnom i radnom procesu. [137]

Najčešće se javlja kao dodatna organizaciona struktura, ponekad i kao primarna, ali u velikom broju slučajeva na nivou organizacije proizvodnje u kompaniji.

4.2.3 Projektno organizaciona struktura

Projektno organizaciona struktura uglavnom je privremena forma organizacije.

Primenjuje se u kompanijama u kojima postoji potreba za poslovnim usmeravanjem i kontrolom izrade proizvoda.[136] Ideja projektne organizacije se zasniva na okupljanju najsposobnijih ljudskih resursa koji su f74raspolaganju kompaniji u svrhu rešavanja složenog zadatka. Po završetku projekta, projektni tim se raspušta. To objašnjava zašto projektna organizacija ima karakteristike fleksibilne organizacije, sposobne da se brzo prilagodi promenama u tehnologiji i zahtevima okruženja svake kompanije. Suštinu projektne strukture čini: izbor menadžera projekta, formiranje projektnog tima, orijentaciju projektnog tima ka ciljevima izrade projekta i raspuštanje projektnog tima nakon izrade projekta.

Projektna organizaciona struktura najčešće je samo interpolirana u5postojeću klasičnu organizaciou strukturu. [137] Privremenog je karaktera, formirana za potrebe realizacije određenog projekta. Međutim, kada se radi o radu na velikim i složenim projektima koji zahtevaju znatne promene u postojećoj organizacionoj strukturi kompanije tada se pristupa formiranju čiste projektne organizacije. [137]

Kompanija koja je otvorena prema promenama, novim tehnologijama i načinima razmišljanja ne ograničava se na organizacionu strukturu koju je formirala na početku svog postojanja, već suprotno tome ona je razvija i koriguje zavisno od potreba i zahteva svog okruženja. Naravno, pri tome se obraća pažnja da promena strukture nije sama sebi svrha, već da je pre svega usklađena sa glavnim ciljevima i promenama stila poslovanja kompanije. To je razlog zbog čega projektna organizaciona struktura predstavlja jedan od oblika organizovanja u savremenim kompanijama koje su usmerene na maksimalno korišćenje znanja i svojih ljudskih potencijala.

4.3 Procesni pristup

Procesno orijentisana kompanija ima imperativ iskorišćavanje svih prednosti menadžmenta poslovnih procesa u kompaniji. U prvom planu suštinu u poslovanju svake kompanije čini znanje koje se nalazi u ljudima, tehnologiji, sredstvima i procesima. Ovde se fokus stavlja na jednom uzajamnom procesu u kome se kompanija mora prilagoditi promenama, jer samu suštinu procesa čini brzina tih promena i mogućnost adaptacije kompanije na te promene. Prema tome, osnova savremenog poslovanja ogleda se u procesima koji definišu skup aktivnosti koje se realizuju u cilju stvaranja izlazne vrednosti za pojedinačnog kupca na tržištu. [98]

Kreiranje procesno orijentisane kompanije predstavlja veliki izazov, bez obzira na veličinu kompanije. U kreiranju takve kompanije prvi korak predstavlja identifikacija primarnih (ključnih) procesa i analiza svih logičkih aktivnosti. Sl50ći korak je kreiranje organizacione strukture. Majchrzak i Wang tvrde da je prosta promena organizacione strukture iz funkcionalnih jedinica u procesno orijentisana odeljenja, nedovoljna da garantuje unapređenje efikasnosti poslovanja kompanije. [138] U kreira50 procesno orijentisane kompanije postoje dva osnovna pristupa. U prvom pristupu organizaciona struktura se u potpunosti orijentiše na poslovne procese kompanije, gde se organizacione jedinice projektuju prema ključnim procesima koji su usmereni ka korisnicima. Drugi pristup podrazumeva postepeno uključivanje poslovnih procesa u postojeću organizacionu strukturu kompanije sve dok se celokupno poslovanje ne zasnuje na dobro utvrđenoj procesnoj osnovi. Za to je zadužen menadžment tim, sa osnovnim fokusom na korisnike. [139]

Pomoću ovog modela, stva50 se struktura koja je u potpunosti orijentisana na korisnike. Primenom informaciono-komunikacionih tehnologija na nivou svakog procesa i

njegovih interakcija ova struktura ima veliku mogućnost adaptacije čestim promenama uslova poslovanja na tržištu. Na nivou svakog procesa definisane su specifične odgovornosti što samo unapređuje kvalitet i brigu o resursima procesa kao i zainteresovanost za ispunjenje unapred definisanih ciljeva kompanije. Ako kompanija nije prilagođena za promene, procese nije moguće organizovati unutar same kompanije. Proces zahteva upotrebu naročito informacionih tehnologija i zato kompanija treba da ovlada znanjima da može da prihvati tu tehnologiju i bude spremna na stalne promene.

4.4 Razvijen informcioni sistem kompanije

Suočena sa dinamičkim uslovima poslovanja kompanije imaju sve veće zahteve za primenom informacionih tehnologija u svom poslovanju. Glavni razlog uvođenja i korišćenja informacionih sistema je usmerenost kompanije na iskorišćavanje informacija koje se javljaju kao rezultat transakcionih obrada podataka s ciljem povećanja njene produktivnosti. Zadatak informacionog sistema je da pruži podršku u korišćenju informacija na tri nivoa u kompaniji: na nivou čitave kompanije, pojedine radne grupe i nivou pojedinca. Informacioni sistem u kompaniji ima zadatak da automatizuje i integriše proizvodne i poslovne procese kao zamenu za ručno izvršavanje tih poslova.

Možemo zaključiti da je primetan veliki kvalitativni napredak, od informacionih sistema u kome se samo prate poslovni procesi pa sve do sistema koji je orijentisan na unapređenje efektivnosti menadžmenta kompanije. Osnova su komunikacije koja smanjuje i neutralizuje zavisnost menadžera nekih organizacionih celina od informacija iz drugih organizacionih celina u kompaniji. Informacije postaju svima dostupne i koriste se u svrhu optimalnog poslovanja kompanije. Dalje, informacioni sistemi su generatori pouzdanih informacija koje su potrebne menadžerima za donošenje poslovnih odluka i kao takvi predstavljaju pomoćno sredstvo za kreiranje strategije kompanije.

4.4.1 Razvoj informacionih sistema

Kompanije treba uvek da budu na usluzi kupcima, drže korak sa konkurencijom, kako bi bile u stanju da donese odluke u realnom vremenu. Na dobijanje kvalitetnih informacija prema potrebama kompanije, utiče stepen organizovanosti i uređenosti kompanije i primena savremenih informacionih tehnologija.[140] Prisutna je svest u kompanijama da praćenje napretka i ugradnja savremenih dostignuća informacionih tehnologija direktno utiče na povećanje poslovne uspešnosti. Zato se kontinuirano vrši reorganizacija poslovanja kompanija u skladu sa razvojem informacionih tehnologija.

U početku je primena informacionih sistema bila usmerena na obradu transakcije. [135] Tokom prvih decenija 21. veka informacioni sistemi evoluiraju i počinju da služe rukovodstvima kompanija za podršku prilikom poslovnog odlučivanja, dok danas integrisani softverski paketi potpomognuti bazama znanja i metodama veštačke inteligencije vrše simulaciju zaključivanja i ponašanja eksperata u kompanijama. Sam tok razvoja poslovnih informacionih sistema može se podeliti na: transakcioni informacioni sistem, sistem za podršku u odlučivanju i ekspertni sistem.

4.4.2 Transakcioni informacioni sistem

Ovaj sistem možemo nazvati klasični informacioni sistem. On predstavlja osnovni informacioni sistem kompanije, a njegova karakteristika je da podržava svakodnevne poslovne transakcije i aktivnosti u kompaniji.

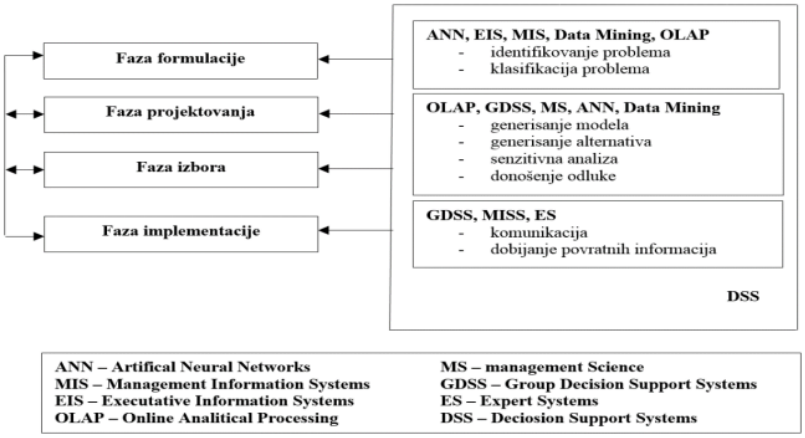
Ovakav sistem počiva na *client-server* arhitekturi kao osnovi za obradu podataka,

dok se manipulacija podataka vrši u domenu transakcija. Ovakva arhitektura se odvija u mrežnom okruženju (*LAN*, *WAN*, Internet), kroz definisane mrežne protokole (*Novell*, *TCP/IP*) pri čemu se svaki tip mrežne arhitekture karakteriše nekim specifičnostima promene. Transakcioni sistemi u kompanijama omogućuju izradu detaljnih izveštaja o dnevnim transakcijama, omogućuju izradu raznih pregleda i sadržaja knjigovodstvenih promena. Međutim, transakcije prikupljene tokom dužeg vremenskog perioda u bazi podataka klasičnog informacionog sistema mogu se procesuirati na takav način da identifikuju pokazatelje nekih trendova u nekom vremenskom periodu. Time se omogućava sveobuhvatniji uvid u poslovne aktivnosti kompanije. Ovde se već može govoriti o nadogradnji klasičnog transakcionog informacionog sistema.

4.4.3 Sistemi za podršku odlučivanju

Sistemi za podršku odlučivanju (engl. *Decision Support Systems – DSS*) predstavljaju informacione sisteme, koji su slični i komplementarni standardnim informacionim sistemima i osnovna uloga im je da podržavaju poslovne procese donošenja odluka u kompanijama. Ovi sistemi mogu da se posmatraju i kao simbioza informacionih sistema, kroz primenu niza funkcionalnih znanja i tekućih procesa donošenja odluka.[141] Pojava ovakvih sistema koji su namenjeni slabo struktuiranim problemima, kao i uključivanje „mekih" podataka u modele za optimizaciju, pružaju suštinski nov pristup poznatim konceptima informacionih sistema. Korisniku sistema za podršku odlučivanja sada je konačno omogućeno da uprosti model pomoću kog rešava realni problem u situacijama gde je to potrebno, zadržavajući pritom njegovu realnu složenost u onim aspektima koje detaljno analizira. [142]

Oni podržavaju sve faza procesa odlučivanja u kompaniji počevši od faze formulacije problema, preko faze projektovanja, faze izbora, pa sve do implementacije. U tom smislu Turban i Aronson [143][144][145][146] objedinjuju primenu raspoloživih alata za podršku odlučivanju sa odgovarajućim fazama procesa odlučivanja (slika 15).



Slika 15. *Kompjuterska podrška fazama procesa odlučivanja u kompaniji*
Izvor: [147]

Sistemi za podršku u odlučivanju treba da pruže menadžerima vremenski odgovarajuće informacije, koje će biti tačne, relevantne i kompletne. Sistem mora da da prikaz informacije u adekvatnoj formi, kako bi bila laka za razumevanje i upravljanje. Informacija prikazana sistemom može biti rezultat ili može biti dobijena iz spoljašnih izvora. Osnovna funkcija sistema za podršku u odlučivanju jeste podrška kod donošenja

strateških odluka kompanije.

Svaki obrađeni podatak u transakcionom delu informacionih podsistema postaje mogući gradivni element kod kasnijih analiza podataka koje su važne ukoliko se posmatraju sa stanovišta sistema za podršku u odlučivanju. [147] Ovi sistemi se prvenstveno vezuju uz strateški nivo upravljanja kompanijom, međutim, ponekad mogu imati i značajan uticaj na niže nivoe menadžmenta. Oni tako grade most između viših i nižih nivoa upravljanja u kompaniji (slika 16).



Slika 16. *Interakcija sistema za podršku odlučivanju i informacionih podsistema u kompaniji*
Izvor: [147]

Svaki ovakav sistem može se posmatrati kao specifičan sistem koji obuhvata elemente rudarenja podataka, statistike, veštačke inteligencije, matematike, menadžmenta i ostalih područja koja vode ka ostvarivanju definisanog cilja. Za ispunjavanje svojih složenijih zadataka u odnosu na transakcione sisteme, sistema za podršku u odlučivanju koristi se dostignućima razvoja informacione tehnologije. Osnovu sistema za podršku odlučivanju čine softverski sistemi koji imaju pristup velikim bazama podataka, iz kojih izvlače sintetičku informaciju u obliku i formatu pogodnom za dati nivo odlučivanja.

Oni se češće koriste na višim nivoima odlučivanja jer su niži nivoi odlučivanja suočeni sa bolje strukturiranim problemima, te su samim tim, u mogućnosti da koriste egzaktne, kvantitativne metode, koje su jednostavne za primenu i daju jednake rezultate. [148] Namena ovih sistema je da podrže, a ne da zamene donosioce odluka. Treba napomenuti da oni ne donosi odluke automatski, već samo obezbeđuju analizu i podršku potrebnu za konkretnije odlučivanje. Obzirom da je sistem namenjen odlučivanju, on sadrži algoritme logičkih i racionalnih procesa putem kojih klasifikuje, upoređuje i formira informacije za odlučivanje. [146] Sistem se može oslanjati na modele koji se izgrađuju na interaktivan način sa korisnikom, podržavajući sve faze odlučivanja i uključujući komponente znanja.

Proces dizajniranja DSS najčešće zavisi od kategorije kojoj sistem pripada, tako da ćemo tabelarno prikazati kategorizacija koju je dao Power, iako postoji više mogućnosti klasifikacije.[140]

Tabela 7. *Kategorije sistema za podršku odlučivanju*
Izvor: [140]

Kategorija	Karakteristika	Primer
Data-Driven	Koristi struktuirane podatke	Data Warehouse
Model-Driven	Koriste modele	Rasporedi
Suggestion	Koriste pravila i relacije	Konsultacije
Group Support	Pomažu komunikaciju i usaglašavanje	Vođenje sastanka
Document-Driven	Koriste nestruktuirane podatke	Web
Inter-Organizational	Podrška komontentima	Pristup kupaca podacima
Functional-Specific	Podrška specifičnim sistemima	Vazduhoplovni, bankarski
Web-Based	Podrška svim DSS	Intranet

DSS koji su zasnovani na podacima (engl. *Data-Driven, DSS*) ističu pristup i manipulisanje struktuiranim podacima u velikim bazama (engl. *data warehouse*), koje sadrže kako interne tako i eksterne podatke kao važan segment rada sa takvim sistemima. Velike baze podataka, odnosno *data warehouse* sistemi omogućavaju efikasan pristup podacima primenom računarskih alata prilagođenih specifičnim namenama kao i primenom opštih alata koji obezbeđuju dodatnu funkcionalnost. *Data-Driven DSS* u kombinaciji sa *OLAP* alatima pružaju visok stepen funkcionalnosti jer omogućavaju i efikasnu analizu velike kolekcije istorijskih podataka.

Sistemi koji koriste finansijske, reprezentacione i optimizacione modele predstavljaju DSS sisteme bazirane na modelima (engl. *Model-Driven, DSS*). Njihova glavna odlika je da akcenat stavljaju na izgradnju i proučavanje modela. Kompleksne analize zasnovane su na modelima koje je moguće izvršiti pomoću OLAP sistema (hibridnih DSS sistema), koji objedinjuju modelovanje, pretraživanje velike količine podataka i mogućnost sumiranja podataka. Oni koriste podatke i parametre obezbeđene od strane donosioca odluka, ali obično nisu naročito orijentisani na podatke.

Sugestivni DSS (engl. *Suggestion DSS*) zasnovani su na *data mining* alatima kao i ekspertnim sistemima. Primenom *data mining* alata analitičarima se sugerišu veze koje postoje među podacima. Ekspertni sistem može sugerisati ali i pokrenuti izvršavanje neke akcije za menadžera. Sugestivni DSS se još nazivaju i DSS koji su bazirani na znanju.

DSS zasnovani na dokumentima (engl. *Document-Driven DSS*) orijentisani su na pretraživanje i upravljanje nad nestrukturiranim podacima kao što su dokumenti i *Web* strane. Glavni zadatak ovih sistema je efikasno pretraživanje. Predstavljaju skup različitih tehnologija smeštanja i obrade nestrukturiranih podataka, u cilju pružanja što efikasnije pretrage i analize dokumenata.

Grupni DSS (engl. *Group DSS, GDSS*) je tip DSS koji uključuje grupno odlučivanje zasnovano na principu usaglašavanja. Ovaj DSS treba kategorizovati kao specifični tip DSS jer uključuje upotrebu specifičnih informacionih tehnologija za kolaborativni rad, ali i efektivan sistem komunikacija što obezbeđuje mogućnost distribuiranog rada.

Inter-organizacioni DSS (engl. *Inter-Organizational DSS*) je relativno nova kategorija DSS. Internet pruža komunikacione linkove za različite tipove inter-organizacionih sistema uključujući i DSS. Oni omogućavaju udaljenim korisnicima da pristupe intranetu kompanije i ukoliko su za to ovlašćeni koriste određene DSS servise.

Funkcionalno specifični DSS (engl. *Function-Specific DSS*) predstavlja sistem koji je specijalno dizajniran da podrži određene poslovne funkcija i tipova poslovanja. Ovi sistemi se obično dizajniraju namenski, za određene zadatke mada se po svojoj prirodi mogu svrstati u neku od glavnih kategorija DSS.

Web orijentisani DSS (engl. *Web-Based DSS*) se implementiraju upotrebom *Web* tehnologija. Menadžerima i poslovnim analitičarima obezbeđuju upotrebu DSS alata koristeći *veb pretraživače*. Ovakvi DSS omogućuju velikom broju menadžera da korišćenjem *web pretraživača* u mrežnom *klijent-server* okruženju donose pojedinačne ili grupne odluke, ali i da pristupaju skladištu podataka kao delu DSS arhitekture.

Uključivanjem DSS u proces odlučivanja doprinosi se povećanju efikasnosti ovog procesa. Alter u [149], navodi sledeće prednosti korišćenja sistema za podršku odlučivanju:

- povećanje pojedinačne efikasnosti,
- ekspeditivnost u rešavanju problema,
- olakšavanje međusobne komunikacije,
- promovisanje učenja i vežbanja,
- povećanje kontrole u kompaniji.

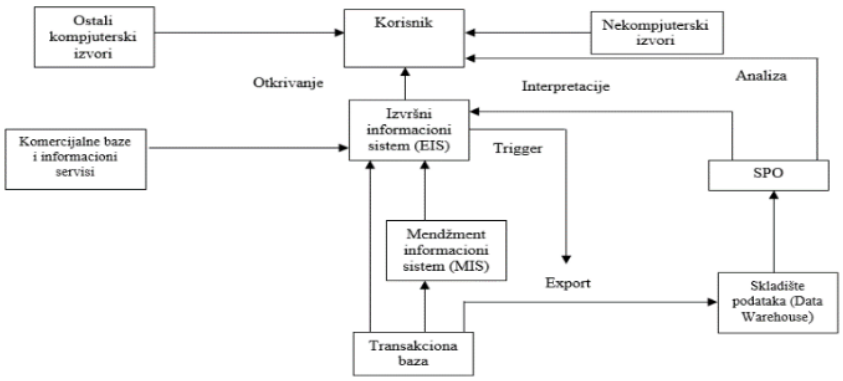
Ipak, u odredenim situacijama, pored prednosti DSS mogu izazvati i negativne posledice. Povećanje stepena kontrole može biti i kontraproduktivno ako se pojedinci na rukovodećim mestima u kompaniji osete ugroženim od upotrebe DSS.

4.4.4 Izvršni informacioni sistemi i izvršni sistemi podrške

Izvršni nivo u kompanijama i njegov opseg zadataka često nije pokriven DSS sistemom. Ukoliko su izvršnom menadžeru kompanije potrebne informacije za donošenje odluka na svom nivou, on mora da ih zatraži od analitičara ili lica iz strateškog menadžmenta kompanije. Tako se pojavljuje problem definisanja zahteva i međusobnog razumevanja, ali i neblagovremenost traženih informacija. Odavde proizilazi potreba za postojanjem jednog sistema koji bi predstavljao *front-end* nivo za DSS i čiji bi zadatak bio da ubrza odgovor na situacije izvršnog odlučivanja koje zahtevaju brzinu i efikasnost. Sistemi ovakvih karakteristika su poznati pod nazivom izvršni DSS (engl. *Executive Information Systems, EIS*, tj. *Executive Support Systems, ESS*).

Izvršni informacioni sistem (engl. *Executive Information System, EIS*) predstavlja sistem čiji je osnovni zadatak da obezbedi tekuće i odgovarajuće informacije menadžerima koji donose izvršne odluke u mrežnom okruženju kompanije. U stvari, EIS predstavlja alat pomoću kog se dobija zbirni izveštaji koji su namenjeni izvršiocima.

Sa druge strane, izvršni sistemi podrške (engl. *Executive Support Systems, ESS*) predstavljaju sveobuhvatne sisteme za podršku odlučivanju koji prevazilaze granice EIS, jer uključuju komunikacije, *office automation*, podršku analizi podataka i inteligentne komponente (slika 17).



Slika 17. *Izvršni sistem za podršku: Integrisanje EIS i DSS*
Izvor: [150]

Ovde možemo zaljučiti da EIS predstavlja računarski sistem koji ispunjava informacione potrebe krajnjih izvršilaca u kompanijama. Pruža brz pristup pravovremenim informacijama i direktan pristup upravljačkim izveštajima. Kao takav, EIS je blizak korisniku (engl. *user-friendly*), grafički je podržan, obezbeđuje izveštavanje o izuzecima i ima mogućnost dobijanja dodatnih detalja nekog izveštaja na osnovu izabrane dimenzije izveštavanja (engl. *drilldown*). Obezbeđuje povezivanje na Internet *on-line* servisima ili putem *e-maila*. Osnovne karakteristike EIS se mogu razvrstati na sledeći način:

- *drilldown,*
- kritični faktori uspeha (engl. *Critical Sucess Factors, CSF),*
- statusni pristup podacima,
- analiza,
- izveštavanje o izuzecima,
- upravljanje informacijama,
- komunikacije.

Danas se oni koriste za detekciju problema, identifikaciju povoljnosti, predviđanje trendova i donošenje odluka zasnovanih na činjenicama. Obzirom da prvenstveno prikazuju zbirne podatke i izveštaje, EIS izvršiocima pružaju imogućnost uvida u detaljne podatke. Osnovna svrha korišćenja EIS je unapređenje kvaliteta i kvantiteta informacija potrebnih na izvršnom nivou što uključuje:

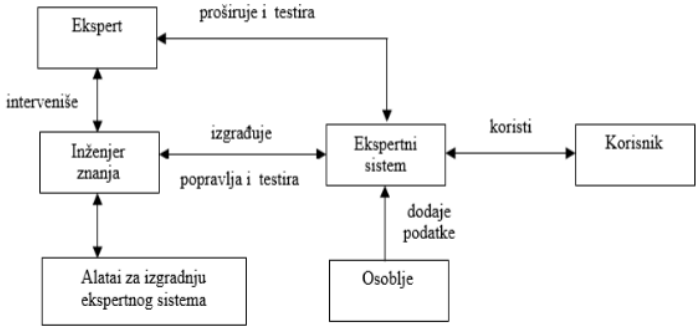
- poboljšanje pravovremenosti informacija,
- efikasan pristup operativnim podacima,
- brži pristup eksternim bazama podataka,
- dobijanje sadržajnijih i relevantnijih informacija.

Najčešća upotreba EIS je u sledećim domenima: podrška donošenju odluka kroz pružanje aktuelnih i tačnih podataka u smislenom formatu; planiranje u pogledu definisanja plana rada, organizacije sastanaka i dr. Pored toga, EIS unapređuju performanse izvršnih poslova obezbeđujući komunikacije, povećavajući efektivnost i efikasnost izvršioca. Redukuju broj sastanaka i utrošeno vreme, omogućavaju izvršno

planiranje, organizovanje i kontrolu i usmeravaju pažnju izvršioca na otkrivene probleme.

4.4.5 Ekspertni sistemi

Sveukupnost procesa izgradnje ekspertnog sistema u literaturi se naziva i inženjerstvo znanja i predstavlja posebnu vrstu interakcije izmedu kreatora ekspertnog sistema – inženjera znanja, i jednog ili više lica koja su eksperti u odredenoj problemskoj oblasti za koju se ekspertni sistem kreira (slika 18). U procesu kreiranja ekspertnog sistema uključeni su: ekspert, inženjer znanja i korisnik. U celom procesu važno mesto zauzima i alat za kreiranje ekspertnog sistema.



Slika 18. *Učesnici u izgradnji ekspertnog sistema*
Izvor: [150]

Kao alat koji treba da simulira znanje eksperta, ekspertni sistemi mogu da se definišu kao programi koji upotrebljavaju ljudsko znanje radi rešavanja problema koji zahtevaju ljudsku inteligenciju. Jednu od najpotpunijih definicija za ekspertni sitem dao je Fajgenbaum sa Univerziteta Stenford: *Ekspertni sistemi su integralni računarski programi koji koriste znanje i postupke zaključivanja da bi rešili probleme koji su kompleksni, te zahtevaju znatnu ljudsku stručnost i veštinu. Kombinovanje znanja i mehanizma zaključivanja za rešavanje tog problema može rezultirati modelom koji simulira najboljeg stručnjaka u toj oblasti*. [151]

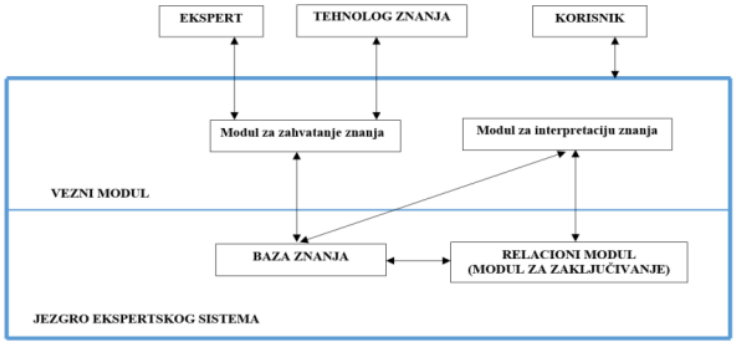
Ekspertni sistemi predstavljaju inteligentne računarske programe koji svoj rad zasnivaju na znanju i postupcima zaključivanja u procesu rešavanja problema za čije je rešavanje potreban visok stepen stručnosti i iskustva iz domena kome se ekspertni sistem obraća. Oni predstavljaju sledeći korak u razvoju informacionih sistema. U odnosu na baze podataka kojima se koriste transakcioni sistemi i bazom modela koju koristi sistem za podršku u odlučivanju, oni poseduju bazu znanja i metode za nadogradnju informacija. Ovi sistemi obezbeđuju predviđanja i odgovor na pitanja tipa „što ako" (engl. *what if*), kao i elemente komunikacije sa ekspertom za neko određeno područje. Ekspertni sistemi predstavljaju najvišu evoluativnu fazu informacionih sistema i predstavljaju najvažnije proizvode koji služe za podršku poslovnog menadžmenta.

Performanse ekspertnog sistema zavise od kvaliteta znanja koje je ugrađeno u njega. Znanje je smešteno u bazi znanja ekspertnog sistema i razlikuju se dva tipa znanja:

- znanje koje se zove činjenicama datog domena i
- heurističko znanje.

Osim znanja, ES zahteva i postupak zaključivanja ali i način za opisivanje znanja u računaru koje ES treba da poseduje, i to na logički struktuiran način tako da sa njima

računar može lako da manipuliše, kao i skup odgovarajućih struktura podataka.



Slika 19. *Osnovna arhitektura ekspertnih sistema*
Izvor: [152]

Svaki ekspertni sistem satoji se iz tri dela: baza znanja, mehanizam zaključivanja i korisnički interfejs (slika19). Baza znanja (engl. *knowledge base*) sadrži znanje eksperta u struktuiranom formatu.[152] Mehanizam zaključivanja (engl. *inference engine*) na osnovu zahteva korisnika i znanja koje se nalazi u bazi rešava korisnički zahtev, tj. pronalazi upravo ono znanje koje je potrebno korisniku. Ima dve osnovne uloge. Prva uloga je da ispituje postojanje određenog znanja u bazi znanja na osnovu korisničkog zahteva i stvara novo znanje na osnovu baze znanja i korisničkog zahteva kada je to potrebno i moguće. Druga je da u zavisnosti od zahteva korisnika koji korisnik najčešće iznosi u iteracijama mehanizmi uređuju redosled kretanja po bazi znanja. Odgovori korisnika na pitanja ekspertnog sistema direktno utiču na način na koji se pretražuje baza znanja. Korisnički interfejs treba da obezbedi jednostavnu komunikaciju između sistema i korisnika tako što će omogućiti jednostavnu upotrebu ekspertnog sistema i kvalitetnu interpretaciju rezultata.

Tabela 8. *Osnovne komparativne razlike DSS i ES*
Izvor: [150]

Karakteristika	DSS	ES
Cilj	poboljšanje strukture odlučivanja	
Predmet	slabo strukturirani problemi	dobro strukturirani problemi
Ko formira odluku?	čovek i/ili sistem	sistem
Metod manipulacije	numerički	simbolički
Domen problema	kompleksni	integralni
Tip problema	ad hoc, pojedinačni	repetitivni
Sadržaj baze podataka	činjenična znanja	proceduralna i činjenična znanja
Sposobnost rezonovanja	nema	da, ograničeno
Sposobnost objašnjenja	ograničena	da
IZLAZ	podaci kao podrška odlučivanju	zaključa (odluka)

Važna karakteristika ekspertnih sistema je i ekspertiza tzv. visokog nivoa. Osobina mogućnosti predviđanja ogleda se u tome da ekspertni sistem može poslužiti kao model za rešavanje problema u nekoj oblasti koji će, pružati odgovore na zadate probleme i ukazivati kako će se ti odgovori menjati zavisno od novih situacija. Još jedna važna karakteristika je i mogućnost obučavanja.

Prednosti primene ekspertnih sistema ogledaju se u: postojanosti, prenosivosti, pouzdanosti i ceni sistema.

Ekspertni sistemi mogu zavisiti i od brzine njihove integracije sa tradicionalnim metodama obrade podataka, kao što su baze podataka, jezici IV generacije i slično. Oni treba da se razumeju kao standardni deo alata koji se upotrebljavaju u razvoju složenih softverskih proizvoda, tj. da budući softverski proizvodi budu na neki način inteligentni.

Tabela 9. *Razlika između konvencionalnih programa i ekspertnih sistema*
Izvor: [150]

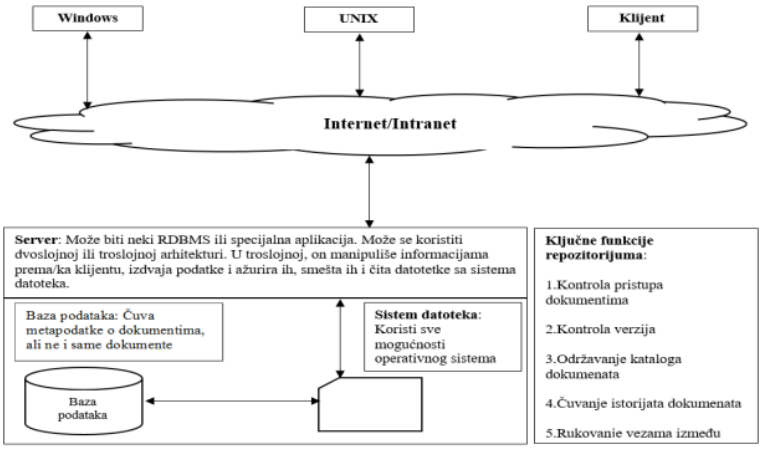
Konvencionalni program	Ekspertni sistem
predstavlja i algoritamski koristi podatke, ponavljajući proces	predstavlja i heuristički koristi znanje, proces zaključivanja
efikasno manipulisanje velikim bazama podataka	efikasno manipulisanje velikim bazama znanja
znanje i metodi korisničkog znanja su izmešani	model rešavanja problema se pojavljuje kao baza znanja, a njom upravlja odvojeni deo – mehanizam zaključivanja (interpreter pravila)
znanje je organizovano u dva nivoa – podaci i program	znanje je organizovano bar u tri nivoa – podaci, baza znanja i mehanizam zaključivanja
u slučaju novog znanja potrebno je reprogramiranje	novo znanje se dodaje bez reprogramiranja, proširivanjem baze znanja

Zanimljiv pravac razvoja ekspertnih sistema predstavljaju i tzv. sistemi za isporuku znanja (engl. *knowledge delivery system*). U suštini oni nisu zasnovani na lancu zaključivanja korišćenjem velikog broja pravila. Ovde se zaključivanje rešava u jednom koraku jer se za svaku moguću premisu vezuje odgovarajući zaključak. Brzim pretraživanjem i upoređivanjem zadate premise sa postojećim u bazi znanja, dolazi se do odgovarajućeg zaključka.

4.4.6 Sistemi za upravljanje (menadžment) dokumentima

Sistemi za upravljanje dokumentima (engl. *Document Management Systems, DMS*) predstavljaju skup tehnologija koje obezbeđuju jednostavan rad sa bilo kojim elektronskim i kompleksnim dokumentima. Osnovnu strukturu DMS čine tri celine (slika 20):

- repozitorijum dokumenta (engl. *document repository*),
- mehanizam protoka posla (engl. *workflow mechanism*),
- tehnologija pretraživanja i indeksiranja (engl. *index and search technology*).



Slika 20. *Osnovna struktura sistema za upravljanje dokumentima*
Izvor: [150]

Zavisno od proizvođača dizajn DMS može biti dvoslojan ili troslojan. Kod dvoslojne arhitekture (sa bazom podataka), klijent obavlja veći deo posla nego u troslojnoj, gde server sa repozitorijumom obavlja najveći deo posla. U bazi podataka se nalaze samo podaci o lokaciji dokumenta, što je u stvari veza baze i sistema datoteka. Serverska aplikacija vodi računa o konzistentnosti. Baza podataka sadrži podatke o dokumentima kao što su: autor, datum, naslov, broj verzije i dr. Iz ovog se može zaključiti da su kvalitet i mogućnosti softvera koji služi za kreiranje dokumenta od velikog značaja za čitav DMS sistem.

Repozitorijum dokumenata predstavlja najvažniju komponenta DMS. On upravlja dokumentima. Osnovne funkcije su mu: bibliotekarske usluge, kontrola verzija i upravljanje vezama između dokumenata i njihovih sadržavnih delova. Postoji u formi posebne aplikacije ili u vidu mehanizma ugrađenog u bazu podataka. U potpunosti indeksira tekstove dokumenta, što olakšava pretraživanje i daje preciznije odgovore na upite, koji sa svoje strane mogu da se bolje i preciznije struktuiraju.

Mehanizam protoka procesa može u potpunosti da eliminiše zastoje u prenosu dokumenta ako se dobro koncipira i primeni. Obezbeđuje reviziju dokumenata na paralelan način, a zajedno sa repozitorijumom objedinjava kompletnu istoriju revizija. Mogu da obaveste korisnike o pojavi nove verzije dokumenta. Ne manje važna je i funkcija konverzije dokumenata kreiranih u jednom ili u drugom, željenom formatu.

Tehnologija pretraživanja i indeksiranja zavisi od toga da li će se koristiti aplikacija za vođenje repozitorijuma ili će se koristiti funkcije ugrađene u bazi podataka. Korišćenje standardnih i kvalitetno strukturiranih dokumenata na osnovu definisanih postupaka kreiranja, ažuriranja, pregledanja i arhiviranja obezbeđuje uspešno rukovanje informacijama na maksimalno jednostavan i efikasan način.

Osnovni principi rešenja DMS su: jednostavnost, brzina, efikasnost i bezbednost. Potencijalne dobiti uvođenjem sistema za upravljanje elektronskim dokumentima su:

- efikasno pretraživanje i pribavljanje potrebnih dokumenata,
- prikupljanje kolekcija dokumenata sa srodnim informacijama,
- podrška za razmenu podataka,

- centralizacija arhive,
- bolja podela poslova,
- podrška za rad više učesnika,
- automatske procedure za vođenje radnih tokova (engl. *workflow*),
- dobijanje znanja o prethodnim radnim procesima i opštim izvorima informacija,
- transparentna sledljivost dokumentacije,
- standardizacija poslovanja,
- veća preglednost poslovanja i
- smanjena administracija kroz integraciju proizvodnje dokumenata i njihovim upravljanjem.

Postoji široka lepeza DMS softvera, kako po mogućnostima koja su na raspolaganju, tako i po programerskim rešenjima, korisničkom interfejsu i cenama. Da bi se ostvario osnovni cilj pri projektovanju svakog od njih usvojen je određeni metodološki pristup, a kod svih je obavezno postojanje nekoliko osnovnih funkcija kao i određenih standarda.

Najvažniji standard koji definiše funkcionalne karakteristike sistema za upravljanje dokumentima je međunarodni standard *180 GES 82045*. Namena mu je pre svega za uređivanje informatički podržanih sistema za elektronsko upravljanje dokumentima (engl. *Electronic Document Management Systems – EDMS*) ili sistema za upravljanje podacima o proizvodima (engl. *Product Data Management Systems – PDMS*) u pogledu upravljanja, pronalaženja, skladištenja i arhiviranja dokumenata, kao i da obezbedi osnovu za razmenu dokumenata.

Potreba za ovakvim sistemima se javlja posebno u okviru državnih organa i prepoznata je u gotovo svim državama sa razvijenom informatičkom infrastrukturom. Da je u većini država ovaj problem shvaćen ozbiljno, govori i činjenica da je razvijan zasebno u svakoj državi i u opštem slučaju nije dostupan izvan državnih institucija.

Primetno je konstantno povećanje primene DMS sistema koji zauzimaju sve važnije mesto među poslovnim rešenjima koje svakodnevno obezbeđuju unapređenje efikasnosti u poslovanju kompanija.

4.5 Informacioni sistemi za kreiranje znanja u kompanijama

Uspeh svake kompanije sve više zavisi od njene sposobnosti da kreira, sakupi, sačuva i distribuira znanje. Znanje postaje centralno produktivno i strategijsko sredstvo u svakoj kompaniji i sa njime one postaju efektnije i efikasnije u korišćenju svojih resursa. Kroz različite mehanizme organizacionog učenja kompanije kreiraju i sakupljaju znanje. Kreiranjem novih standardnih operativnih procedura i poslovnih procesa, kompanije isprobavaju različite alternative i pažljivo upoređuju planirane aktivnosti i povratnu vezu od klijenata i okruženja kao celinu. Kompanije koje imaju jake mehanizme učenja brzo detektuju pokazatelje iz okruženja i odgovaraju na njih, čime sebi stvaraju šansu da opstanu na tržištu i ostvare profit. Sam menadžment znanja unapređuje sposobnost kompanije da uči iz njenog okruženja i da svojim poslovnim procesima pridoda znanje gde važnu ulogu igra informaciona tehnologija.

Većina vrsta informacionih sistema olakšavaju tok informacija i menadžment znanja u kompanijama. Pored unapređenja sposobnosti informacionih tehnologija da identifikuju pokazatelje iz okruženja i daju odgovore na njih, oni direktno podržavaju organizaciono učenje i upravljačke zadatke u kompaniji. Sistemi kancelarijske kolaboracije (engl. *Office Automation System – OAS*), sistemi grupne kolaboracije, sistemi za dizajniranje (engl. *Computer Aided Design – CAD*), kao i aplikacije veštačke inteligencije naročito su korisni za menadžment znanja. Oni se fokusiraju na definisanje i organizovanje baze znanja kompanije i na podršci poslovnih procesa vezanih za informacije i znanje.

Kreiranjem, čuvanjem, kodifikovanjem i distribucijom eksplicitnog i implicitnog znanja, informacioni sistemi mogu unaprediti organizaciono učenje. Informacije koje se jednom prikupe i organizuju u informacionom sistemu mogu se koristiti prema potrebi bez vremenskog ograničenja. Kako bi znanje najboljih praksi stajalo na raspolaganju zaposlenima, sve te najbolje prakse, najuspešnija rešenja ili metode rešavanja problema moraju biti razvijena u samoj kompaniji. Znanje se u kompaniji može čuvati u memoriji organizacije, a ono bi se kasnije koristilo za obučavanje budućih zaposlenih i za pomoć menadžerima prilikom donošenja poslovnih odluka. Sačuvano znanje iz prošlosti kompanije u memoriji organizacije može biti upotrebljeno za donošenje poslovnih odluka i u druge razne svrhe.

U tabeli 10 prikazan je pregled informacionih sistema koji podržavaju aktivnosti menadžmenta znanja u kompaniji. Specijalizovane sisteme kao što su sistemi za dizajniranje CAD (engl. *computer-aided design – CAD*) i sistemi virtuelne stvarnosti koriste visoko stručni kadrovi i eksperti u kompanijama kako bi kreirali nova znanja i integrisali ga u kompaniju. Sistemi grupne kolaboracije podržavaju kreiranje i deljenje znanja između lica koja rade u grupi. Sistemi veštačke inteligencije prihvataju i čuvaju novo znanje i obezbeđuju kompanijama i menadžerima kodifikovano znanje koje se može ponovo koristiti od strane drugih zaposlenih u kompaniji. Korišćenje ovih informacionih sistema zahteva IT infrastrukturu koja omogućava korišćenje moćnih računara, mreža, baza podataka, softvera i internet alata. [153]

Tabela 10. *Aktivnosti i sistemi za menadžment znanja*
Izvor: [154]

Aktivnosti Menadžmenta znanja kompanije	**IS za menadžment znanja kompanije**
Kreiranje znanja	**Kancelarijski IS** (obrada teksta, desktop i web izdavaštvo, elektronski kalendari, desktop baze podataka) **CAD sistemi** **Sistemi virtuelne realnosti**
Čuvanje i kodifikovanje znanja	**Sistemi veštačke inteligencije** (ekspertni sistemi, neuronske mreže, fuzzy logika, genetski algoritmi, inteligentni agenti)
Deljenje i distribuiranje znanja	**Sistemi grupne kolaboracije** (e-mail, telekonferencije, groupware sistemi, intranet sistemi)

Kancelarijsko poslovanje u kompanijama uzima veliki deo poslova koji je vezan za podatke, informacije i znanje,uključujući i poslove koje izvršavaju rukovodioci prilikom donošenja odluka. Glavnu ulogu ukoordinaciji toka informacija i znanja kroz celu kompaniju imaju kancelarije. U tabeli 11 prikazane su aktivnosti koje se izvršavaju u administrativni radnici u kancelarijama i aplikacije IT za povećanje njihove produktivnosti.

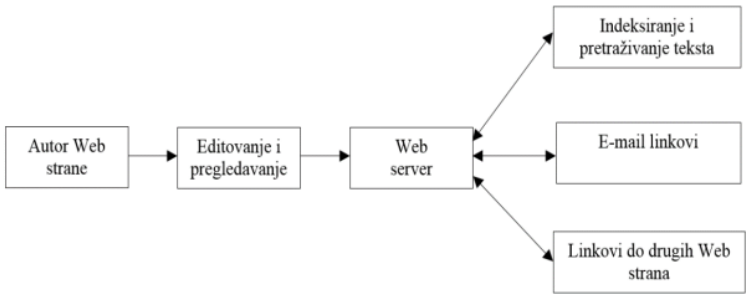
Tabela 11. *Kancelarijske aktivnosti i IT*
Izvor: [154]

Kancelarijska aktivnost	**Informacione tehnologije**
Menadžment dokumentima	Obrada teksta, desktop izdavaštvo, snimanje *(imaging)* dokumenata, *web* izdavaštvo, upravljanje radnim tokovima *(worflow)*
Planiranje obaveza	Elektronski kalendari, softver radnih grupa, intranet
Komunikacija	*E-mail*, *voice mail*, digitalni *answering* sistemi, softver radnih grupa, intranet
Menadžment podacima	*Desktop* baze podataka, *spreadsheet* softver, laki za korišćenje interfejsi od *mainframe* baza podataka

Okruženje koje je bazirano na umreženim digitalnim uređajima na kojima se izvršavaju različiti tipovi aplikacija i čijom se primenom povezuju profesionalne, administrativne i upravljačke radne grupe predstavljaju idealnu varijantu za kancelarijsko poslovanje u kompanijama. Često se zanemaruje segment upravljanja dokumentima, kada se razmatraju projekti menadžmenta znanja. To zanemarivanje može uzrokovati ostvarivanja velike uštede u troškovima obrade dokumenata, izvlačenje neophodnog znanje iz tih dokumenata i na kraju ostvarivanje velike konkurentske prednosti na tržištu. Efikasan menadžment dokumentima neophodan je u onim oblastima poslovanja i poslovnim aktivnostima kompanija koje su intenzivno praćene velikim brojem raznovrsnih dokumenata.

Automatizacija upravljanja elektronskim dokumentima može se implementirati u kompanijama pomoću sistema koji treba da obezbedi alate za kreiranje, smeštanje, lako lociranje i skladištenje dokumenata. Isto tako, ovaj sistem bi trebalo da obezbedi sprovođenje određenog stepena kontrole nad dokumentima. On vrši integraciju čitave IT u jedinstvenu arhitekturu koja bi pratila dokument od njegovog kreiranja, do njegove distribucije.[155]

Zaposleni mogu objaviti informacije korišćenjem *web* alata u internoj informatičkoj infrastrukturi kompanije. Tako informacije postaju deljiv resurs, jer postaju dostupne unutar kompanije putem standardnog *web* pretraživača. Prednost primene web tehnologija za objavljivanje informacija ogleda se u mogućnosti indeksiranja u cilju bržeg pristupa i povezivanja sa drugim dokumentima (slika 21). [155]



Slika 21. *Web publikovanje i menadžment dokumentima*
Izvor: [155]

U kreiranju i integrisanju novog znanja u kompanijama pored kancelarijskih sistema i sistema za dizajniranje (CAD), koriste se i sistemi virtuelne stvarnosti. Arhitektura ovih sistema obezbeđuje korisnicima specijalizovane alate, kao što su grafički alati i alati za vizuelizaciju, analitički alati, alati za modelovanje i simulaciju,

komunikacioni alati i alati za upravljanje dokumentima.

Sistemi za dizajniranje (engl. *Computer Aided Design – CAD*) vrše automatizaciju kreiranja i revidiranja dizajna proizvoda korišćenjem računara i sofisticiranog grafičkog softvera. Dizajner korišćenjem CAD radnih stanica, kreira prototip proizvoda, jer se dizajn može lako testirati i menjati na računaru. Mogućnost da obezbedi specifikacije dizajna za obradu i proizvodni proces CAD softvera, isto tako štedi vreme i novac kompaniji.[130]

Sistemi virtuelne stvarnosti imaju mogućnosti vizualizacije, prevođenja i simulacije koje su mnogo veće nego kod CAD sistema. Oni koriste interaktivni grafički softver za kreiranje računarski-generisanih simulacija koje su blizu stvarnosti, da korisnici mogu da poveruju da učestvuju u stvarnim situacijama. Virtuelna stvarnost ima primenu u oblastima obrazovanja, nauke i biznisa.[156] Aplikacije virtuelne stvarnosti razvijene su za *Web*, korišćenjem standarda pod nazivom VRML (engl. *Virtual Reality Modeling Language – VRML*), što predstavlja programski jezik za modelovanje virtuelne stvarnosti. Standard VRML je skup specifikacija za interaktivno trodimenzionalno modelovanje na *World Wide Web* koje se koriste za organizovanje više tipova medija, uključujući animacije, slike i audio zapise, kako bi se korisnici stavili u simulirano realno okruženje. Nezavistan je od hardverske platforme, može da funkcioniše na desktop računaru i zahteva manju propusnu moć mrežnih komunikacija (engl. *bandwidth*).

Menadžeri u savremenim kompanijama postaju svesni da je znanje, kao nematerijalno sredstvo i resurs, od izuzetnog strategijskog značaja. Ulaganja u informacione tehnologije za menadžment znanja se povećavaju, uz očekivanje da će dovesti do veće konkurentnosti i profita. Kompanije koje u svom redovnom poslovanju kreiraju puno dokumentacije, treba da se posebno angažuju na iskorišćavanju znanja i intelektualnih resursa koji su inkorporirani u tim dokumentima. Da bi se to postiglo, potrebna su ulaganja u informacione sisteme za kreiranje znanja u kompanijama, kao što su kancelarijski sistemi, CAD sistemi i sistemi virtuelne stvarnosti.

4.6 Struktura Interneta i e-dimenzija menadžmenta znanja

Produktivan menadžment znanja zahteva kombinovanu primenu ljudskih resursa i tehnologija. Ljudski resursi su neophodni u cilju razumevanja, sinteze i interpretacije raznih vrsta nestruktuiranog znanja, dok računarski i komunikacioni sistemi omogućavaju njegovo prikupljanje, prenos i eksploataciju. Računarski i mrežni sistemi i njihova upotreba (*e-mail*, zajednički softver, Internet, intranet) omogućavaju jednostavnu i brzu razmenu znanja bez obzira na udaljenost korisnika. Nove tehnologije nude znatno bolje modele za saradnju. One omogućavaju interakciju bez obzira na vreme i prostor što predstavlja asinhronu saradnju. Pravi izazov za informacione tehnologije predstavlja stvaranje informacionog sistema koji će biti upotrebljen za prenošenje, podelu i korišćenje znanja kompanije.

Nezaobilazna činjenica u svim segmentima savremenog poslovanja je Internet. Paradigma uspeha poslovanja svake kompanije uvek je podrazumevala neophodnost prilagođavanja promenama u okruženju u pogledu izbegavanja mogućih opasnosti i iskorišćavanju prilika. Kompanije koje su na vreme prepoznale potencijal Interneta danas u najvećoj meri koriste web tehnologije kao nezaobilazan element razvoja svog poslovanja. Sa razvojem internet infrastrukture kreiraju se nove dimenzije koje veoma utiču na poslovanje savremenih kompanija. Razvoj informaciono-komunikacionih tehnologija i Interneta sve više utiče na afirmaciju kvalitativnih i neopipljivih parametara kao što su: ideje, inovacije, intelektualni kapital i znanje, povezanost sa kupcima, njihovo

zadovoljstvo kvalitetom proizvoda i uslugama. One unapređuju kvalitet komunikacije i smanjuju troškove kompanija. Razvoj informacionih tehnologija i Interneta pojačao je potrebu, kao i snagu za menadžment znanja. Razvoj informacionih tehnologija danas omogućava prikupljanje i skladištenje znanja, ali i kreiranje novih znanja potrebnih za razvoj poslovanja kompanija. Ovde moramo konstatovati da tehnologija još uvek ne može da zameni vrednost i potrebu direktne komunikacije, barem ne još uvek u delu kada je u pitanju deljenje znanja zasnovanog na iskustvu. Međutim, tehnologija može uspešno pomoći u posredovanju i olakšavanju kreiranja mreže zasnovane na znanju ljudi.

Razvoj Interneta predstavlja neophodnu osnovu za razvoj globalnog tržišta znanja na kome se sreću oni koji znanje nude i oni koji kupuju znanje. Obzirom na dostupnost informacija, povećava se i uticaj pojedinaca na poslovanje kompanija. Znanje jednog čoveka može imati presudan uticaj u preduzetništvu koje svoje poslovanje zasniva na znanju. Naravno, taj proces treba biti dopunjen i Internetom. U dosadašnjem poslovanju velike kompanije su svoju moć održavale menadžmentom informacija u i van svojih kompanija. Međutim, danas to više nije moguće. Stručnjak za intelektualni kapital Edvinsson, navodi da budućnost poslovanja savremenih kompanija počiva na razmeni znanja, podjednako kao i na deljenju znanja. [104]

Razvoj tržišnih mehanizama kao što su berze na Internetu, predstavljaju veliku vrednost jer stvaraju produktivna tržišta znanja. One omogućavaju „kupcima i prodavcima" znanja razmenu svoje robe prema utvrđenim cenama na osnovi navedenih tržišta. Prema tvrdnjama Edvinssona,[157] ova navedena tržišta će postati treća generacija berze i aukcije za recepte znanja. Ta berza će omogućiti kupovinu i prodaju znanja i iskustva putem računarskih mreža.

Prednost i glavna odlika znanja je da je ono obnovljiv izvor koji se ne troši, već naprotiv njegovom upotrebom njegova vrednost raste što ga izdvaja u odnosu na druge robe koje se razmenjuju na berzama. U tom pogledu, Internet može omogućiti laku i sveobuhvatnu razmenu znanja i oslobađanje vrednosti i potencijala individua. Pomoću Interneta obezbeđuju se novi oblici društvene interakcije, aktivnosti i organizacije, zahvaljujući osnovnim karakteristikama kao što su rasprostranjena upotrebljivost i pristup.

4.7 Organizacija koja uči

Kao jedan od savremenih koncepata za rešavanje problema upravljanja kompanijom u smislu sticanja i održavanja konkurentskih prednosti na tržištu pojavila se ideja o organizaciji koja uči.[158] Savremena globalna i digitalizova ekonomija nameće efektivno korišćenje znanja kao produktivniji i postojan izvor konkurenstke prednosti. [159] U okruženju koje karakterišu veoma naglašeni trendovi kao što su globalizacija i sve snažniji konkurentski pritisak, kompanije akcenat stavljaju na konkurentnost u znanju. U tom okruženju jedina kompanija koja može da obezbedi opstanak i da se uspešno bori sa konkurencijom je organizacija koja uči. [160]



Slika 22. *Model učenja*
Izvor: [161]

Slater i Nar[illegible] smatraju da je organizacija koja uči kompanija koja izgrađuje svoju prednost na tržištu upotrebom intelektualnih resursa svojih zaposlenih i stalnim procesima učenja na individualnom, grupnom i organizacionom nivou. [162] Elinger i ostali tvrde da kompanije na taj način ostvaruju bolje organizacione performanse i transformišu se u organizacije koje uče. [163]

U operativnom smislu, Marsick i Watkins kažu da je organizacija koja uči kompanija u kojoj zaposleni međusobno rade na zajedničkim vizijama, analiziraju okruženje i prikupljene informacije, stvarajući tako novo znanje koje primenjuju za kreiranje inovativnih proizvoda i usluga namenjenih da zadovolje p[illegible]ebe korisnika. [164] Peters tvrdi da organizacija koja uči podržava individualno učenje i ima zajedničku viziju i duboke korporativne vrednosti, ali je i u mogućnosti da prepozna važnost kontinuiranog učenja, kreativnog i sistemskog razmišljanja. [165] Tokom svog istraživanja, više autora je pokušalo da opiše i definiše organizaciju koja uči. Pregled definicija organizacije koja uči dat je u tabeli 12.

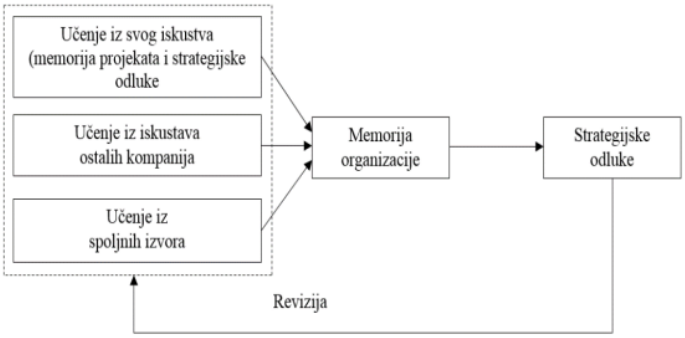
Tabela 12. *Pregled definicija „Organizacije koja uči"*
Izvor: [165]

Autor	Definicija
Senge (1990)	Organizacija koja uči je organizacija u kojoj ljudi kontinuirano proširuju svoje kapacitete u cilju postizanja željenih rezultata, gde se neguju novi obrasci razmišljanja, gde se teži zajedničkoj viziji i gde ljudi stalno uče kako zajedno da uče.
Pedler, Burgojn i Bojldejl (1991)	Kompanija koja uči je organizacija koja olakšava učenje svih njenih članova i stalno se transformiše, kako bi ostvarila svoje strateške ciljeve.
Vitkins i Marsik (1993; 2003)	Organizacija koja uči je ona koja kontinuirano uči i transformiše se... Organizacija koja uči proaktivno koristi učenje na integrisani način, kako bi podržale i podstakle rast pojedinaca, timova i čitavih organizacija, kao i institucija i zajednica sa kojima su povezane.
Garvin (1993)	Organizacija koja uči je ona koja proaktivno kreira, stiče i prenosi znanje, i menja svoje ponašanje na osnovu novog znanja i uvida.
DiBella i Navis (1998)	Organizacija koja uči je okarakterisana kao ona koja ima sposobnost da se prilagodi promenama u svom okruženju i da upotrebi prethodno iskustvo menjajući organizaciono ponašanje.
Markuardt (2002)	Organizacija koja uči je kompanija koja uči efektno i kolektivno, i stalno se tranformiše u cilju boljeg upravljanja i korišćenja znanja, ovlašćuje ljude unutar i izvan organizacije da uče dok rade; koristi tehnologiju kako bi povećala učenje i proizvodnju.

Piter Senge se smatra pravim začetnikom teorije o organizaciji koja uči. [160] On tvrdi da će najuspešnije kompanije biti one koje imaju svojstva organizacije koja uči, odnosno koje imaju sposobnost da uče brže od svoje konkurencije čime će ostvariti i održati svoju konkurentnu prednost na tržištu. Prema njegovom mišljenju u vreme sve veće povezanosti sveta i dinamičnih i složenijih poslova, više nije dovoljan jedan strateg u kompaniji koji uči za celu kompaniju i na čije odluke se čeka. U novije vreme, na tržištu mogu da se održe samo one kompanije koje uspevaju na svim nivoima da pokrenu svoje zaposlene, da uče i maksimalno iskoriste svoje mentalne i fizi[illegible] potencijale. [160] Organizacija koja uči treba da bude takva da u njoj zaposleni stalno razvijaju svoje sposobnosti stvaranjem rezultata koje žele, u kojoj se neguju novi obrasci, a kolektivne ambicije slobodno postavljaju i u kojoj zaposleni kontinuirano uče kako da uče zajedno. [160]

Organizaciono učenje u svakoj kompaniji predstavlja namerni ili nenamerni organizacioni proces, koji omogućava akviziciju pristupa i reviziju memorije organizacije i na kraju vodi ka konkretnoj akciji kompanije – donošenju odluke. [166] Danas znanje i učenje mora da bude deo organizacione kulture i organizacionih procesa u kompaniji.

Kompanije koje ne implementiraju menadžment znanja danas su marginalizovane i preti im propadanje, jer se osnove nove ekonomije baziraju na sticanju znanja i učenju, odnosno, kako upotrebljavati i realizovati menadžment znanja. Velika konkurencija globalnog tržišta naterala je kompanije da odbace poznate stereotipe i tradicionalne načine poslovanja. Prinudila ih je na novi pristup stvaranje pozitivne atmosfere i kreativnog radnog okruženja čime podstiču svoje zaposlene na razmenu ideja i znanja i definisanje organizacione kulture koja se zasniva na učenju.



Slika 23. *Proces organizacionog učenja*
Izvor: [166]

U organizacijama koja uče razvijaju se strategije i sistem vrednosti u svrhu zadržavanja postojećih i privlačenju novih zaposlenih koji su eksperti u svom području rada. Savremene informaciono-komunikacione tehnologije, ekspertni sistemi i Internet direktno doprinose boljem menadžmentu znanja i bržoj podeli i razmeni znanja.

Organizaciju koja uči karakteriše mogućnost brže adaptacije na promene u okruženju i visok nivo inovacija vezanih za procese rada, proizvode i tehnološka rešenja. [167] U takvim organizacijama svi članovi organizacije se podstiču na liderstvo. [168] [169][170]. Time se obezbeđuju veštine, kompetencije i klima koja ispunjava postojeće zahteve korisnika, lakše se prilagođava na izmenjene zahteve i pomaže u planiranju ska na nove segmenate i tržišta [55][162]. Takođe, organizacije koje uče stvaraju balans između ličnih i profesionalnih razvojnih potreba zaposlenih i kako bi se oni podstakli da koriste nove veštine na inovativne načine. [160] Sve je veći naglasak na sposobnosti koje doprinose ostvarivanju boljih organizacionih performanse. [163]

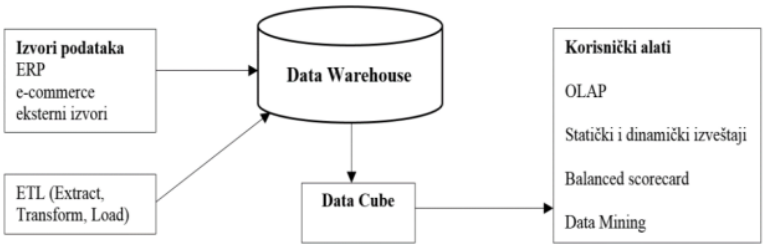
Na kraju možemo zaključiti, da mali broj kompanija ima kapacitete za realizaciju menadžmenta znanja i njegovom iskorišćavanju kao svoje konkurentske prednost na tržištu. Pasivno i neiskorišćeno znanje nema udela u stvaranju nove vrednosti i razvijanju intelektualnog kapitala kompanije. Ako se koristi intelektualni kapital kompanije n stvara nove vrednosti i podiže tržišnu cenu kompanije. Svaka organizacija koja uči, uvažava i poznaje svoju sakrivenu imovinu, stvara uslove i organizacionu kulturu, motiviše zaposlene na učenje, timski rad, razmenu znanja i iskustav i razvoj kreativnosti i inovacija. Time ona kvalitetno sprovodi menadžment znanja sa krajnjim ciljem postizanja konkurentske prednosti na globalnom tržištu, a znanje i intelektualni kapital postaju njeni osnovni ekonomski resursi.

4.8 Sistem poslovne inteligencije

Pored standardnih parametara, danas najveću konkurentsku prednost kompanija predstavlja zajedničko znanje i veštine zaposlenih koji danas predstavljaju ključne resurse

za donošenje kvalitetnih poslovnih odluka. Uvođenjem informacionih sistema u kompanije došlo je do prikupljanja velikih količina podataka. Prikupljanjem podataka nastajale su nove baze podataka u kojima se našao potencijal za poboljšanje poslovnog odlučivanja. Ipak, za dolaženje do informacija iz tih podataka, a time i novih znanja, javila se potreba razvijanja alata koji bi taj proces omogućili i ubrzali. Tako je počeo razvoj poslovne inteligencije (engl. *Business Intelligence, BI*) koja omogućava prikupljanje i analizu podataka i delovanje na osnovu poslovnih informacija. Na taj način se doprinosi lakšem rešavanju upravljačkih problema i donošenju najboljih poslovnih odluka. Ovakvi sistemi izvorno su namenjeni donosiocima odluka.

U literaturi postoje različite verzije definicija poslovne inteligencije. Izdvojićemo nekoliko. Kimball i Ross označavaju poslovnu inteligenciju kao opšti termin za opis uticaja unutrašnjih i spoljašnjih informacija kompanije za donošenje boljih poslovnih odluka [171]. Suknović i Delibašić smatraju da je poslovna inteligencija skup informacionih tehnologija i organizacionih pravila ali i znanja i veština zaposlenih u organizaciji udruženih u stvaranju, zapisivanju, integraciji i analizi podataka, sa ciljem da se dođe do potrebnog znanja za donošenje odluke [152] Larson u svojim istraživanjima poslovnu inteligenciju podrazumeva kao pružanje tačnih i korisnih poslovnih informacija donošenje odgovarajućih poslovnih odluka. [172] Barry shvata poslovnu inteligenciju kao sticanje i iskorišćavanje znanja zasnovanog na činjenicama u svrhu unapređivanja strateške i taktičke poslovne prednosti na tržištu. [173] Rainardi smatra da je poslovna inteligencija skup metodologija i platformi za skladištenje podataka (engl. *Data Warehousing*)[174], on-line analitičku obradu (engl. *On-Line Analytical Processing, OLAP*), izveštavanje, statističke analize, predviđanja i otkrivanje znanja u bazama podataka (engl. *Data Mining*). Svi oni omogućavaju kompanijama kreiranje korisničkih upravljačkih informacijama iz podataka o poslovanju. [175]



Slika 24. *Konceptualna arhitektura poslovne inteligencije*
Izvor: [174]

Razvojem tehnologije promenjen je način donošenja odluka u kompanijama. Sa automatizacijom procesa sve više podataka postaje dostupno. Poslovna inteligencija u suštini predstavlja osnovnu tehnološku strukturu koja pruža poslovnim subjektima potpuno upravljanje informacijama obezbeđujući im mogućnost boljeg pozicioniranja na tržištu [176]. Kao takva je inteligentan sistem planiranja i analize događaja u kompaniji. Osnovna karakteristika ovih sistema je dostupnost informacija o kupcima, dobavljačima, procesima i njihovim međusobnim odnosima. Na taj način se omogućuje proaktivan način vođenja kompanije, sa izradom više scenarija i predviđanjem budućnosti kako bi kompanija bila pripremljena na svaku moguću situaciju na tržištu. [177]

Zbog nerazumevanja stvarne prirode poslovne inteligencije i njenih dometa, ne postoji dovoljno poznavanje ni razumevanje svih oblika u kojima se ona danas pojavljuje. Razloge takve raznolikosti leže u činjenici da su funkcionalnosti alata za poslovnu

inteligenciju poslednjih dvadeset godina evoluirale u nekoliko smerova. Ipak, danas uglavnom ne postoje arhitekture ovih sistema koje bi mogle kvalitetno integrisati sve te funkcionalnosti i alati koji bi bili sposobni da podrže sve stilove poslovne inteligencije. [178]

Imajući u vidu razvoj aplikacija i tehnologije, mogu se identifikovati pet dominantnih stilova poslovne inteligencije:

- poslovno izveštavanje,
- OLAP kocke,
- *ad hoc* upiti i analize,
- rudarenje podataka (engl. *Data Mining*),
- alarmni alati i sistemi ranog obaveštavanja. [179]

Većina dostupnih alata i tehnologija usmerena je ka jednom ili više od navedenih pet stilova poslovne inteligencije, što manjoj meri zadovoljava rastuće potrebe i ambicije korisnika, a samim tim motiviše proizvođače softvera na razvoj snažnijih i kompleksnijih rešenja. Kompanije danas zahtevaju metodologiju koja integriše sve navedene stilove poslovne inteligencije u bilo kakvoj kombinaciji aplikacija. [180] Teži se arhitekturi koja omogućava:

- jednostavnu integraciju svih stilova poslovne inteligencije i njihovih funkcionalnosti,
- upotrebu jedinstvenog okruženja za pristup softverskim alatima koji omogućuju bilo kojiod tih stilova,
- dostavu i isporuku rezultata putem jedne platforme, koja će se bazirati na jedinstvenoj ontologiji podataka i unifikovati meta podatke, ali i pružati zadovoljavajući nivo bezbednosti i podržavati različite profile korisnika. [181]

Kao gotov proizvod sistem poslovne inteligencije ne postoji, već njegovi proizvođači nude tehnološke platforme i znanja za ugrađivanje. [178] Uvođenje sistema poslovne inteligencije zahteva obaveznu podršku upravnog dela kompanije.

5. Rudarenje podataka / Data Mining

Korporativne strategije zavise od informacione infrastrukture koja obuhvata različite tehnologije koje omogućavaju kompanijama da čuvaju, analiziraju i manipulišu velikim količinama podataka. [182] Njihovi izvori mogu biti različiti (interni, eksterni, analitički), dok su podaci najčešće atributivni ili numerički. Mogu se odnositi i na činioce koje određuju poslovanje kompanije, interne procedure, na klijente kompanije, poslovanje konkurencije i poslovnu okolinu. Međutim, ovakvi podaci nemaju veliku upotrebnu vrednost iz razloga što su neobrađeni, neadekvatno strukturirani i različitih su formata. Neophodno je izvršiti njihovu pripremu i analizu na osnovu kojih će se doći do znanja koja kompaniji mogu obezbediti poslovni uspeh.

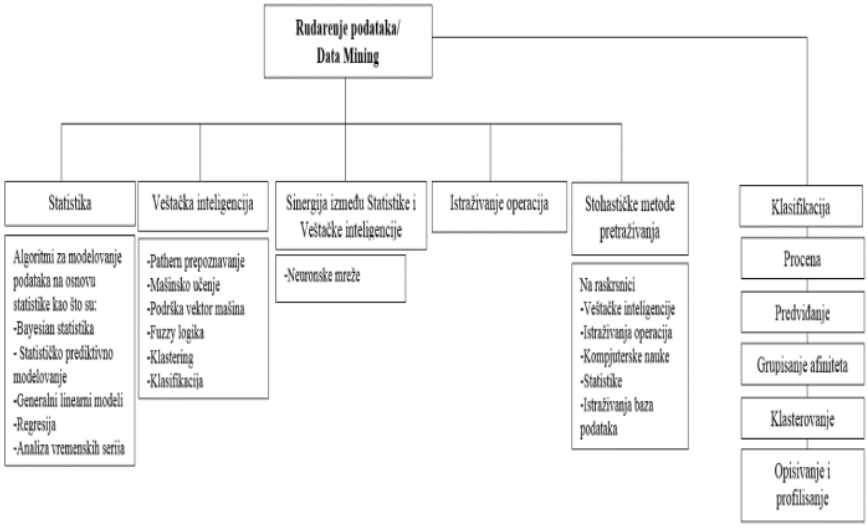
Analize se vrše od strane posebno razvijenih programa i sistema. Rudarenje podataka je jedna od tih novih metodologija kojom se otkrivaju vredni podaci u velikim količinama podataka i bazama podataka kompanija kako bi se donele efikasne poslovne odluke.

5.1 Pojam rudarenja podataka

Rudarenje podataka (engl. *Data Mining*) i njegova primena u otkrivanju znanja jedna je od novih tehnika koje pr[illegible]aju neizostavan deo savremene analize podataka. Predstavlja pronalaženje šablona u podacima kako bi se dobile informacije koje se mogu upotrebiti u svrhu odlučivanja ili stvaranja neke od[illegible]tene vrednosti u kompaniji. Rudarenjem podataka otrivaju nove i korisne informacije iz podataka na temelju otkrivanja ponavljajućih šablona. Otkrivanje novih informacija zasniva se na brojnim algoritmima razvijenim u oblasti veštačke inteligencije i mašinskog učenja a koji čine njegovu tehničku osnovu. [183]

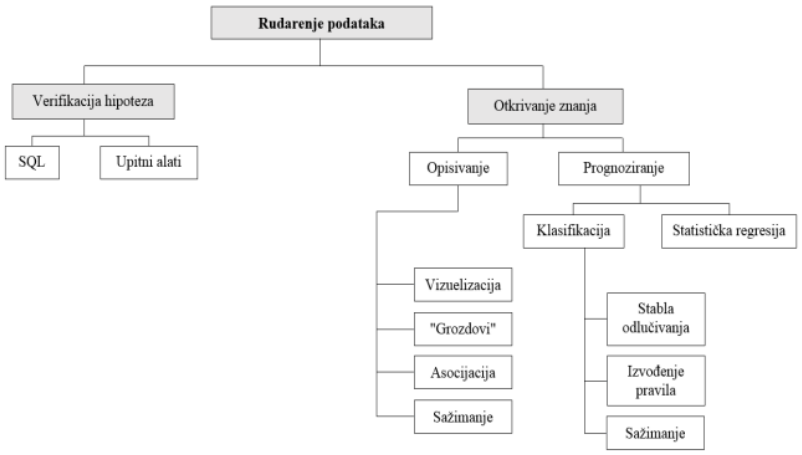
U literaturi se mogu identifikovati nekoliko definicija rudarenja podataka. Pang-Ning Tan ga definiše kao automatsko otkrivanje korisnih informacija u velikim repozitorijumima podataka. Pomoću tehnika rudarenja podataka pronalaze se nepoznati korisni obrasci. [184] Po Davidu J. Handu, rudarenje podataka predstavlja analizu (često velikih) posmatranih podataka u cilju identifikacije veza između podataka na način koji je razumljiv i odgovarajući vlasniku podataka. [185] Suknović [152], pak posmatra rudarenje kao otkrivanje znanja u bazama podataka, identifikaciji interesantnih informacija ili šablona sadržanih u velikim bazama podataka.

Rudarenje podataka se može definisati kao otkrivanje znanja u bazama podataka, analiza šablona, uočavanje međusobnih veza u podacima, obrada podataka, i dr. Kompanija IBM [132] definiše rudarenje podataka kao proces identifikacije prethodno nepoznatih a korisnih informacija iz velikih baza podataka i njihovo ko[illegible]ćenje za potrebe donošenja ključnih poslovnih odluka. Fayyad ga definiše kao netrivijalni proces identifikacije validnih, novih, potencijalno korisnih i razumljivih obrazaca u podacima [186]. Feruzza to vidi kao skup metoda korišćenih u procesu detekcije znanja kojim identifikuje prethodno nepoznate veze i obrasce unutar podataka. [187][188][189][183][190][191]



Slika 25. *Rudarenje podataka / Data Mining*
Izvor: [193]

Iz navednog možemo zaključiti da je rudarenje podataka skup metoda i tehnika, realizovanih u softveru, kako bi se otkrile skrivene informacije u podacima. Ono predstavlja multidisciplinarno područje koje uključuje: baze podataka, ekspertne sisteme, teoriju informacija, statistiku, matematiku, logiku i čitav niz drugih oblasti (slika 25).



Slika 26. *Taksonomija rudarenja podataka*
Izvor: [193]

Mnogi stručnjaci smatraju da je rudarenje podataka sinonim za otkrivanje znanja iz podataka (engl. *Knowledge Discovery from Data*) dok drugi na to gledaju samo kao na ključni korak u procesu otkrivanja znanja. Otkrivanje znanja u bazama podataka (engl. *Knowledge Discovery in Database, KDD*) Fayyed je definisao kao proces identifikacije važećih, novih, potencijalno korisnih i na kraju razumljivih obrazaca u podacima.[192]

Termin rudarenja podataka često se izjednačava sa dva različita procesa: otkrivanje i prognoziranje znanja (slika 26).

5.1.1 Zadaci (problemi) rudarenja podataka

Uslov za efikasnije poslovno odlučivanje kompanija je posedovanje preciznih podataka o sopstvenom i poslovanju konkurenata što je imalo presudan uticaj na razvoj rudarenja podataka. Kvantifikacijom svih aspekata poslovanja korporacija nastale su ogromne baze podataka, tako da primena kompleksnih kalkulacija na taj veliki broj podataka prestavlja osnovni zahtev rudarenja podataka. Poslovna primena rudarenja podataka fokusirana je pre svega na izvlačenju podataka važnih za poslovanje, kao i konkretnih informacija koje imaju neposredan uticaj, dok opšti principi i dublja značenja imaju sekundarni značaj.[194] Najčešći i najpoznatiti zadaci rudarenja podataka su:

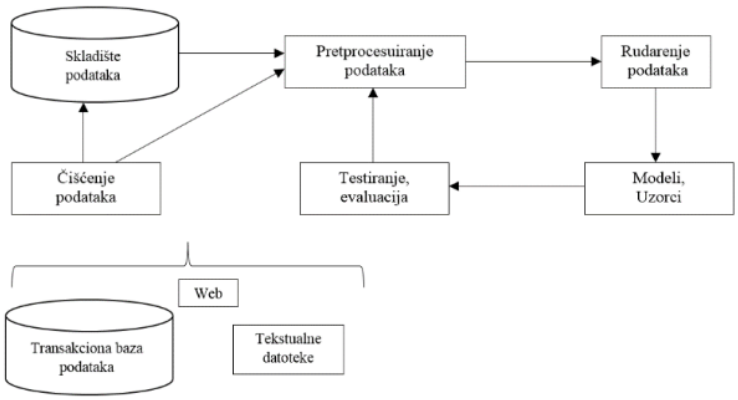
- klasifikacija – raspoređivanje elemenata u predodređene grupe ili klase,
- redukcija – uočavanja veza i zavisnosti između atributa ili objekata,
- estimacija – procena vrednosti egzogene promenljive na osnovu endogenih promenljivih koje su zabeležene u sistemu,
- predviđanje – vrši se procena stanja koje se očekuje u nekom trenutku u budućnosti,
- asocijacija – pronalaženje pravila u bazi podataka i
- klasterovanje – grupisanje elemenata ili opservacija u klase sličnih objekata.[194]

Rudarenje podataka se primenjuje u različitim slučajevima, od kojih se izdvajaju sledeći [152]:

- analiziranje podataka i podrška odlučivanju (analiza tržišta),
- analiziranje prodaje i segmentacije tržišta, analiza potrošačke korpe, povezane prodaje (analiza rizika),
- prognoze, analiza konkurencije, kvalitetna kontrola (dijagnostika nepravilnosti),
- ostale oblasti primene kao što su tekst mining (news grupe, e-mail, dokumenti), web analiza, inteligentni upiti.

5.1.2 Rudarenje podataka i otkrivanje znanja

Zbog brzog rasta količina podataka u bazama podataka, bilo kakva obrada podataka bez upotrebe računara i savremenih metoda i tehnika za analizu je neefikasna i nemoguća. Kako bi se otkrili potencijalni problemi i proširile perspektive, oblast rudarenja podataka zasniva se na savremenim statističkim i matematičkim modelima za analizu podataka o poslovanju kompanija i njihovim klijentima.



Slika 27. *Otkrivanje znanja primenom metoda rudarenja podataka*
Izvor: [178]

Rudarenje podataka može se primenjivati u svim područjima u kojima postoje izazovi za odgovorima, gde se na osnovu podataka mogu otkriti određene pravilnosti, veze i zakonitosti. Imajući u vidu da postoji čitava lepeza faktora koji mogu uticati na neki određeni događaj, odnosno njegov ishod, rudarenje podataka se nameće kao nezaobilazan činilac otkrivanja faktora i njegovih karakteristika u odnosu na ciljano stanje. [195]

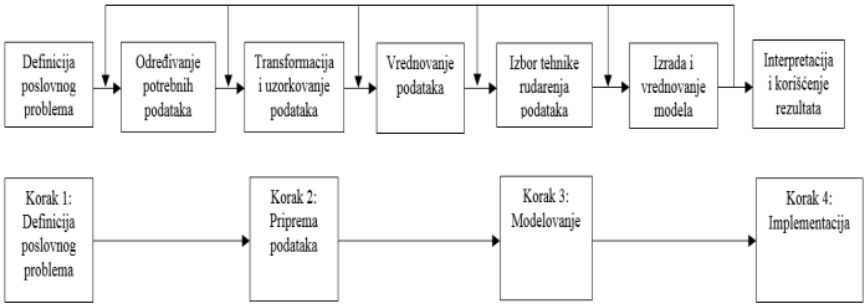
Najbolji rezultati rudarenja podataka dobijaju se balansom između znanja eksperata koji opisuju problem i mogućnostima pretraživanja računara. Proces rudarenja podataka se može kategorisati na dva načina: prediktivno rudarenje podataka, ili deskriptivno rudarenje podataka. Prediktivno rudarenja podataka ima za cilj kreiranje modela koji je izraženu vidu izvršnog koda, a koji se može upotrebiti za izvođenje klasifikacije, predikcije, procene ili drugih sličnih zadataka. Deskriptivno rudarenje podataka kao krajnji cilj ima razumevanje analiziranog sistema uočavanjem obrazaca i veza unutar velikih skupova podataka.

5.1.3 Koraci u procesu rudarenja podataka – otkrivanje znanja

Ne postoji ustaljena i propisana šema po kojoj se realizuje proces rudarenja podataka kada se razmatra šir lepeza tehnika koje se u njemu primenjuju. Poslovne odluke se odlikuju zahtevima da se neki koraci prošire i uđe u njihovu detaljnu analizu, ili da se neki preskoče, jer su suvišni, ili pak da se napravi „korak unazad", radi provere ispravnosti postupka. Ovakav „skok unazad" sve više postaje pravilo nego izuzetak, zbog važnosti dobrog definisanja problema kao i izbora i pripreme podataka, što je teško uraditi na početku samog procesa. Tokom procesa povećava se znanje o poslovnom problemu i podacima. Ipak, to ne znači da je nemoguće dati okvir za realizaciju ovog procesa, već samo ukazuje na činjenicu da je on prilagodljiv potrebama rešenja poslovnog problema. [196]

Osnova okvira za realizaciju rudarenja sastoji se u četiri koraka (slika 28):

- definisanje poslovnog problema,
- priprema podataka,
- modelovanje,
- implementacija (interpretacija i korišćenje rezultata).[197]



Slika 28. *Koraci i faze procesa rudarenja podataka*
Izvor: [197]

Definisanje poslovnog problema je prva faza u procesu rudarenja podataka u kome je potrebno rešiti iskazivanje problema u formi pitanja na koja se po završetku procesa može odgovoriti. Valjan pristup definisanju poslovnog problema je analiza oblasti gde je rudarenje podataka već uspešno korišćeno ranije. U ovoj fazi određuju se lica koja će učestvovati u procesu.

Priprema podataka je druga faza u kojoj se određuju vrste potrebnih podataka prema izvorima u kome se realizuje njihova selekcija i vrednovanje. Obuhvata 60–90% vremena neophodnog za rudarenje podataka. [198] U okviru ovog koraka treba odlučiti koji izvori podataka će biti najpogodniji, i kako će se izvršiti ukrštanje podataka. Ovde se realizuju dva postupka transformacija i uzorkovanje podataka[199] i vrednovanje podataka.

Treća faza procesa rudarenja podataka je modelovanje, a sastoji se u izboru metode rudarenja podataka, izradi i vrednovanju modela. Metode rudarenja podataka se mogu podeliti u tri kategorije: otkrivanje, klasifikacija i predviđanje. [200] Pomoću metoda otkrivanja traže se pravilnosti u podacima bez prethodnog znanja o njihovom obliku. Metode za klasifikaciju variabli koriste se za predviđanje. Klasifikacija se često izvodi pomoću stabla odlučivanja, logističke regresija i neuronskih mreža. Primenom metoda za predviđanje vrednosti omogućava se predviđanje numeričkih vrednosti. Za predviđanje se takođe koriste neuronske mreže, kao i linearna regresija, ali i metode vremenskih serija. Tek nakon njihove primene na konkretnim uzorcima podataka bira se metoda rudarenja podataka. Primena svih ovih metoda bila bi teško moguća bez softvera za rudarenje podataka. Na tržištu postoje brojna besplatna i komercijalna softverska rešenja koja mogu biti zasnovana na više metoda ili biti specializovana samo za jednu. Nakon konstruisanja i primene metoda vrednuju se dobijeni rezultati. Za vrednovanje metode koriste se i podaci za testiranje modela, čime se testira efikasnost modela na podacima koji nisu korišćeni za njegovu izradu.

U završnoj fazi procesa rudarenja podataka izvodi se interpretacija i eksploatacija rezultata. U ovoj fazi ključnu ulogu imaju eksperti pomoću kojih se vrši interpretacija rezultata. Ako se modeli rudarenja podataka implementiraju u informacioni sistem kompanije unapredиće se mogućnost predviđanja odnosa kompanije sa klijentima u budućnosti.

5.2 Priprema podataka za rudarenje

Na uspešnost procesa rudarenja podataka utiču izvori podataka i kvalitet podataka. [201] Podaci se mogu skladištiti u *Excel* datotekama, *ASCII*, *DBF* datotekama i sl., a moguće su i njihove kombinacije. Takođe, rudarenje podataka se može primenjivati na web i tekstualnim podacima. Imajući u vidu planirani cilj analize, javlja se i potreba povremenog povezivanja na sve bitne izvore podataka sa ciljem dobijanja podataka relevantnih za analitički proces. Takvi podaci moraju da prođu kroz postupak čišćenja, pretprocesuiranja i analize relevantnosti atributa.

Priprema podatka je nezaobilazni akspekt u procesu rudarenja podataka koji oduzima najveći deo vremena svakog analitičara. Koliko će se vremena potrošiti za pripremu podataka dosta zavisi od postojanja ili nepostojanja kvalitetnog skladišta podataka (engl. *Data Warehouse*). U skladištu podataka smešteni su integrisani i pročišćeni podaci iz različitih izvora podataka čime analitičar štedi vreme za korake integracije i čišćenja.[202] Alati za pripremu podataka obezbeđuju olakšavanje ovog procesa što značajno ubrzava razvoj modela. Neke od funkcija alata omogućavaju podršku u pripremi podataka. Primena dobrih algoritama za rudarenje podataka na loše pretprocesuirane podatke, ili na „sirove" podatke uvek će na kraju dati loš rezultat.[203]

5.2.1 Pretprocesuiranje podataka

Pretprocesuiranje podataka (engl. *data preprocessing*) i postupci čišćenja podataka daju značajnu ulogu kvalitetu podataka. Pretprocesuiranje podataka podrazumeva pripremu podataka pre primene metoda istraživanja podataka. Primenjuje se radi dobijanja podataka koji više odgovaraju različitim svrhama i potrebama istraživanja podataka. Najznačajniji metodološki postupci pretprocesuranja podataka su: [202]

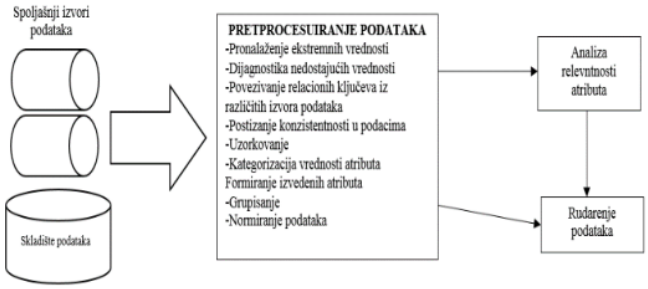
- identifikacija ekstremnih vrednosti (engl. *outliers*),
- identifikacija nedostajućih vrednosti i njihovo predviđanje,
- povezivanje relacionih ključeva iz različitih izvora podataka,
- stvaranje konzistentnosti u podacima,
- uzorkovanje,
- kategorizacija vrednosti atributa,
- kreiranje izvedenih atributa (engl. *binning*),
- grupisanje (kompresija podataka),
- normiranje podataka.

U prepoznavanju podataka mogu nam koristiti i standardne metode deskriptivne statistike, pomoću kojih možemo vršiti procenjivanje osnovne karakteristike čitave populacije. Takođe, analiza korelacionih odnosa i ukrštanja između varijabli obezbeđuju smernice za dublje analize.

5.2.2 Analiza relevantnosti atributa

Nakon pretprocesuiranja podataka, mora se izvršiti provera relevantnosti grupe atributa koja jednoznačno definišu problematiku koju treba rešavati, da li su vrednosti tih atributa grupisane na odgovarajući način, i tražiti opravdanost vršenja analize nad izabranim stepenom granulacije podataka.

Realizacija pretprocesuiranja podataka vrši se u skladu sa ciljevima analize. Ukoliko je potrebno dublje poznavanje podataka može se realizovati i analiza relevantnosti atributa. Razlog procene relevantnosti atributa javlja se iz razloga njene upotrebljivosti i upoznavanja osnovne populacije nad kojom se vrše analize. Može se pokazati da ovakve vrste analiza mogu značajno doprineti u razumevanju odnosa između atributa, a na taj način i izboru adekvatne metode rudarenja podataka.



Slika 29. *Odnos analize i relevantnosti atributa nakon izvršavanja pretprocesuiranja podataka*
Izvor: [193]

Primarni cilj procene relevantnosti atributa u suštini se sastoji na pronalaženju atributa koji imaju slab ili nikakav uticaj na zadati analitički cilj, što može rezultirati njihovom neuvrštavanju u dalje procese analize.

5.2.3 Završni postupci

Razmatrajući kvalitet podataka idealan primer bi mogao da bude slučaj gde kompanija poseduje razvijen sistem skladištenja podataka i da se u njemu nalaze svi relevantni atributi koji su planirani da se koriste u analizama. Krajnji cilj ovog postupka je dobijanje jedinstvene tablice koja treba da sadrži relevantne atribute za traženu analizu. Ako pretprocesuiranje nije realizovano u skladu sa ciljevima analize onda to može dovesti do gubitka detaljnosti podataka i njihove reprezentativnosti.

Kako bi se uočile bitne karakteristike podataka preporučuje se metoda vizualizacije. Ona je usko povezana sa područjem statističke obrade podataka i rudarenjem podataka. Realizuje se iz razloga pronalaženja pravilnosti u podacima, koje već u ovoj fazi analize mogu dati naznake mogućeg rešenja. Grafički prikaz podataka iskorišćava ljudski potencijal za uočavanje uzoraka, izuzetnosti i važnih detalja koji u tabelarnom obliku ne mogu biti lako uočeni. Rezultati rudarenja podataka često se prikazuju 2D i 3D grafikonima, kao i u animacijama. Najveći izazovi prilikom generisanja vizualizacija su: tačnost i skladnost podataka, isticanje korisnih informacija i novog znanja, kao i prilagođenost području.[204]

Glavni pravac razvoja ove oblasti će biti u području dinamičke vizualizacije „živih" tokova podataka, i interaktivnosti, što će korisnicima pružiti veće mogućnosti manipulacije i lakše uočavanje novih informacija. Sa razvojem alata za vizualizaciju podataka, kao i standardizacijom brojnih tokova podataka stvaraju se mogućnosti za povezivanje interdisciplinarnih izvora podataka, a što svakako vodi u novi uvid veza između opisanih pojava od strane izvora. [205]

5.3 Tehnike rudarenja podataka

Rudarenje podataka je primenjivo u svim oblastima koje raspolažu sa velikom količinom podataka, a na osnovu kojih se mogu otkriti određene veze, pravilnosti i zakonitosti. Tehnike koje se koriste odavno su poznate, a to su matematičke tehnike i algoritmi. Bez obzira na to što je rudarenje podataka mlada tehnologija, veoma je važno korišćenje ranijih saznanja. U tom pogledu primenjuju se kombinacije metodolija i tehnika: statistike, mašinskog učenja i baza podataka. [206]

Određeni algoritmi kao što su regresije i stabla odlučivanja dolaze iz oblasti statistike. Neki od njih su preuzeti iz mašinskog učenja i primenjuju se prilikom klasifikacije i regresije, kao i u slučajevima kada su veze između atributa nelinearnog tipa. Prilikom klasifikacije i klasterovanja koristi se genetski algoritam. Naravno, razvijen je i veći broj novih algoritama, metoda i softvera. [183]

Kako bi proces rudarenja podataka bio uspešan, potrebno je precizno formulisati cilj i problem istraživanja. Uspeh je u direktnoj zavisnosti od kvaliteta podataka kojima raspolažemo. Kada je reč o izboru metoda rudarenja podataka, danas na raspolaganju postoji čitav niz metoda. [207]

5.3.1 Metoda regresije

Osnova velikog broja istraživanja predstavlja opis veza između pojava u okruženju što se postiže pronalaženjem formule ili jednačine koja povezuje posmatrane veličine. Identifikacija statističkih veza između pojava obezbeđuje se metodom regresione analize – regresija. To je metoda koja uključuje statističko učenje (engl. *statistical learning*). Pomoću regresije se može kreirati model za predviđanje i ocenjivanje jedne ili više zavisno promenljivih na osnovu jedne ili više nezavisno promenljivih. Problem opisa ovakvih veza svodi se na identifikaciji modela koji povezuje jednu ili više zavisno promenljivih Y_1, Y_2, ... Yp sa jednom ili v nezavisno promenljivih X_1, X_2, ... Xu, pomoću neke funkcionalne zavisnosti. Najčešće je on nepoznat, pa istraživaču ostaj a sam izabere onu koja je po nekom kriterijumu najbolja gde pomažu polinomne, eksponencijalne ili neke druge funkcije. Opšti problem nalaženja funkcije koja dovoljno dobro vrši aproksimaciju dobijenog skupa podataka, često se naziva prilagođavanje krive, tj. određivanje regresione linije.

Pogodna je za opisivanje veza između varijable od primarnog interesa i tzv. prediktorskih varijabli, odnosno, kada se postoje vrednosti koriste za predviđanja ostalih vrednosti. Metode regresije mogu se primeniti za predviđanja kao npr. koliko će profita generisati pojedina kategorija potrošača ili slično. Međutim, većina problema u stvarnom svetu ne predstavlja linearnu projekciju prethodnih vrednosti. Veoma teško je predvideti obim prodaje, cene na berzi ili pad proizvodnje jer sve te vrednosti zavise od kompleksnih interakcija varijabli, pa se tada primenjuju mnogo kompleksnije tehnike, kao što su stablo odlučivanja ili neuronske mreže.

5.3.2 Klasifikacione metode

Klasifikacione metode su namenjene za razvrstavanje entiteta u jednu od nekoliko prethodno definisanih grupa ili klasa. Njima se vrši identifikacija karakteristika koje ukazuju na grupu kojoj pripada svaki pojedinačni slučaj. U postupku rudarenja podataka stvaraju se klasifikacioni modeli kroz ispitivanje prethodno klasifikovanih podataka (slučajeva) i indukcionim traženjem predvidljivih obrazaca.

Klasifikacione metode se najčešće koriste za rudarenje podataka, jer je u ljudskoj

prirodi da stvari oko sebe konstantno klasifikuje i kategorizuje. Klasifikacija nekog objekta zasnovana je na identifikaciji sličnosti sa unapred određenim objektima koji su pripadnici različitih klasa. Sličnost dva objekta definisana je analizom njihovih karakteristika gde se pri tome svaki objekat svrstava u neku od klasa sa određenom tačnošću. Objekti koji se klasifikuju, najčešće se predstavljaju kao n-torke u tabeli ili datoteci. Potrebno je da se na osnovu osobina objekata čija je klasifikacija unapred poznata, napravi model na osnovu koga će se vršiti klasifikacija novih objekata.

Klasifikacione metode se upoređuju i ocenjuju na osnovu sledećih kriterijuma:

- tačnost,
- brzina,
- robustnost,
- skalabilnost,
- interoperbilnost – jasan prikaz i razumevanje rezultata.

5.3.3 Metode klasterovanja

Metoda klasterovanja (engl. *clustering*) predstavlja aktivnost u okviru istraživanja podataka i koristi za grupisanje podataka koji su slični. Spada u grupu tehnika nenadgledanog učenja i omogućava grupisanje instanci u grupe, gde unapred ne znamo koje su sve grupe moguće. Grupe nisu unapred definisane, već se grupisanje vrši na osnovu pronađenih sličnosti između podataka. Tako formirane grupe nazivaju se klasteri. Cilj klasterovanja je da se identifikuju grupe sa značajnim međusobnim razlikama, dok su članovi unutar grupa vrlo slični jedni drugima. [183] U odnosu na metodu opisanu u prethodnom odelju, na početku klasterovanja se ne zna po kojim će atributima podaci biti svrstani u grupe klastera. Postoji niz algoritama za rešavanje ovog problema. Ovde ćemo se osvrnuti samo na *K-means* algoritam i hijerarhijsko klasterovanje. [208]

Osnovna osobina *K-means* metode svodi se na deljenje osnovne populacije na *k* segmenata, pri čemu svaki od segmenata sadrži slične elemente. Sličnost između elemenata se procenjuje na osnovu funkcije udaljenosti. U iterativnim procesima elementi se vezuju uz centralne vrednosti klastera. Ako se posmatra iz perspektive prečišćenih podataka za analizu, klasterovanje svakom slogu dodeljuje vrednost pripadnosti klastera, a može pridružiti i vrednosti udaljenosti od centra klastera. Primenjuje se na jednu dimenziju, ali i u dimenzionalnim prostorima. U tom slučaju potrebno je metodologiju primeniti na svaku dimenziju ponaosob. [209]

Hijerarhijsko klasterovanje se karakteriše grupisanjem objekata u stablo klastera. Zavisno od smera particionisanja, ovo klasterovanje klasifikuje se na klasterovanje od dna ka vrhu (engl. *bottom-up*) i divizijsko klasterovanje (engl. *top-down*). Nedostatak hijerarhijskih algoritama klasterovanja je u nemogućnosti ponavljanja procesa klasifikacije na istom nivou stabla nakon što se izvrši deljenje populacije u klastere. [210]

Osnovna karakteristika algoritama za klasterovanje je da rade samo sa numeričkim vrednostima. Kada se u proces analize uvrste i varijable koje nisu numeričke, prethodno treba izvršiti transformaciju nenumeričkih u numeričke vrednosti. [211] Metoda klasterovanja je pogodna za početnu segmentaciju tržišta. Takođe, klasteri se mogu primeniti i za praćenje trendova tržišnih segmenata, a postoji i niz drugih oblasti na koji se klasterovanje može uspešno primeniti. [212][213] Može se zaključiti da je klasterovanje uspešno onoliko koliko su dobijeni klasteri smisleni i koliko se mogu imenovati.

5.3.4 Neuronske mreže

Primene neuronskih mreža su mnogobrojne i pomeraju granice veštačke inteligencije, računarstva i primenjene matematike. Neuronske mreže u suštini predstavljaju parametrizovanu reprezentaciju koja može poslužiti za aproksimaciju drugih funkcija. Identifikacija odgovarajućih parametara vrši se sistematičnom optimizacijom nekog kriterijuma kvaliteta aproksimacije i može biti računaski vrlo izazovno. [214]

Neuronske mreže (engl. *neural networks*) predstavljaju i tehniku rudarenja podataka predviđenu da deluje slično ljudskom mozgu. Poznato je da ljudski mozak nakon procesa učenja kreira određene pretpostavke na osnovu ranijih zapažanja, te su na ovoj osobini zasnovane neuronske mreže koje predviđaju promene dešavanja u sistemu nakon procesa učenja. U tom smislu, proces rudarenja podataka pomoću podataka koji su već poznati i koji se odnose na vrednosti čija se prognoza traži započinje učenje mreže. Dobijeni rezultati se zatim proveravaju, sve dok rezultati provere ne budu zadovoljavajući. Suština je da se neuronskoj mreži pruže podaci za koje već znamo izlazne vrednosti kako bi na osnovu njih neuronske mreže prepoznale obrasce i pravila. Na osnovu dobijenih obrazaca i funkcija istražuju se ogromne količine podataka koje kompanije poseduju u svojim bazama. [214]

Primenom neuronskih mreža, odnosno nelinearnih modela predviđanja omogućava se modelovanje kompleksnih problema u kojima se može javiti stotine varijabli koje imaju veliki broj interakcija. Biološke neuronske mreže su neuporedivo složenije u odnosu na matematički model koji se koristi u praksi. Osnovna učenja neuronskih mreža su veze između eksperimentalnih uzoraka. Uzorci se klasteruju ili se dva različita tipa uzoraka pridružuju jedan drugome. Ovi sistemi imaju puno širi spektar primene od regresione analize. Bitno je napomenuti da ne postoji jedinstveni model neuronske mreže koji bi se primenjivao na sve vrste problema.

Neuronske mreže, iako najkomplikovanija metoda, daje najtačnije modele. Svoj izlaz temelje na kombinovanju niza ulaza pomnoženih sa odgovarajućim težinama. Kada se projektuje neuronska mreža najpre se određuje struktura (broj neurona i njihove međusobne veze). U cilju predviđanja upotrebom neuronskih mreža potrebno je definisati težine pojednih veza, što se postiže treningom neuronske mreže. Obezbeđuju joj se test podaci i zatim ako je rezultat treninga netačan koriguje se odgovor. Tako se obezbeđuje da neuronska mreža koriguje težine pojednih veza između neurona. Obzirom da neuronska mreža vremenom uči, sa povećanjem broja treninga daje sve tačnije rezultate.

Tabela 13. *Primena neuronskih mreža*
Izvor: [216]

Finansije: – Predviđanje na berzi – Dostojnost kredita – Kreditni rejting – Predviđanje bankrota – Procena vlasništva – Otkrivanje prevara – Prognoza cena – Prognoza ekonomskih indikatora	**Istraživanje podataka:** – Predviđanje – Klasifikacija – Otkrivanje promene i devijacije – Otkrivanje znanja – Modelovanje odziva – Analiza vremenskih sesija
Medicina: – Medicinske dijagnoze – Otkrivanje i evaluacija medicinskih fenomena – Prognoza dužine hospitalizacije pacijenta – Procena cene lečenja	**Prodaja i marketing:** – Prognoza prodaja – Ciljni marketing – Prognoza korišćenja servisa
Industrija: – Upravljanje procesa – Kontrola kvaliteta – Predviđanje temperature i sile	**Operaciona analiza:** – Optimalizacija zaliha maloprodaje – Optimizacija zakazivanja – Menadžersko pravljenje odluka – Prognoza protoka gotovine
Nauka: – Prepoznavanje šablona – Modelovanje fizičkih sistema – Evaluacija ekosistema – Identifikacija polimera – Prepoznavanje gena – Botanička klasifikacija – Procesiranje signala: neuronsko filtriranje – Analiza bioloških sistema – Analiza i identifikacija mirisa	**Menadžment ljudskih resursa:** – Izbor i zapošljavanje – Zadržavanje zaposlenih – Zakazivanje osoblja – Profilisanje osoblja **Energija:** – Prognoza električne opterećenosti – Prognoza energetske potražnje – Kratkoročna i dugoročna procena opterećenosti – Predviđanje indeksa cene gasa/uglja – Sistemi za kontrolu – Nadzor rada hidroelektrana
Obrazovanje: – Predviđanje uspeha studenata – Istraživanje neuronskih mreža – Trijaža fakultetskih prijava	**Ostalo:** – Sporstko klađenje – Odabir pobednika konja i pasa – Kvantitativna prognoza vremena – Razvoj igrica – Optimizacioni problemi, usmeravanje – Procena poljoprivredne proizvodnje

Prednost neuronskih mreža je u laganoj implementaciji i realizaciji na velikom broju paralelnih računara pri čemu svaki čvor istovremeno vrši svoju sopstvenu kalkulaciju. Neuronske mreže su snažan alat, osobito za prognoziranje trendova i predviđanje na bazi istorijskih podataka. Međutim, potrebno je naglasiti da interpretacija neuronskih mreža nije laka, pa one zahtevaju sveobuhvatan trening za osposobljavanje osim za slučajeve rešavanja „malih" problema. [215]

U mogućnosti da se koriste kao proizvoljan mehanizam aproksimacije funkcija koje uče na osnovu podataka glavni je adut neuronskih mreža. Izbor modela zavisi od reprezentativnosti podataka i oblasti primene. Preterano složeni modeli mogu da stvore probleme pri učenju. Svaki algoritam učenja se dobro ponaša sa ispravnim parametrima za treniranje na konkretnom fiksnom skupu podataka.

Problemi na koje se primenjuju neuronske mreže su: [215]

- aproksimacija funkcija ili regresiona analiza, zajedno sa vremenskim serijama,
- klasifikacija, uključujući prepoznavanje šablona i sekvenci,
- procesuiranje podataka, uključujući filtriranje, klasterovanje i kompresiju,
- upravljanje – numeričko računarsko upravljanje.

Postoji nekoliko vrsta neuronskih mreža. Osnovnu varijantu čine neuronske mreže sa propagacijom unapred (engl. *feed forward neural networks*). U obradi slika i drugih vrsta signala, pa i teksta, vrlo su popularne konvolucione neuronske mreže (engl. *convolutional neural networks*). Za obradu podataka, sličnih nizovima promenljive dužine, upotrebljavaju se rekurentne neuronske mreže (engl. *recurrent nerual networks*), dok se za obradu podataka koji se predstavljaju stablima koriste rekuzivne neuronske mreže (engl. *recursive neural networks*), a za obradu podataka koji se predstavljaju grafovima koriste se grafovske neuronske mreže (engl. *graph neural networks*). [216]

5.3.5 Stablo odlučivanja

Jedan od osnovnih pos[103]ka mašinskog učenja je stablo odlučivanja. [217] Kao metoda veoma je popularna zbog svoje jednostavnosti izvođenja i mogućnosti da se rezultat indukcije može prikazati grafički. Dodatna prednost je što se postupak može direktno koristiti za rešavanje problema više klasa. [218] Formiranje stabla odlučivanja predstavlja metodu stv[63]nja klasifikatora iz podataka i jedna je od najčešće korišćenih logičkih metoda. Ono predstavlja hijerarhijski model, koji se sastoji od čvorova i grana. Testiranje atributa se vrši u čvorovima, dok grane predstavljaju sve moguće izlaze za testirani atribut u nekom čvoru.

Kod stabla odluč[39]nja grane predstavljaju moguća alternativna rešenja identifikovanog problema. Koristi se u procesu odlučivanja pri iznalaženju optimalnih rešenja, posebno u uslovima kada pos[39] određene neizvesnosti i rizik, gde je očigledno postojanje više alternativih rešenja problema koji je predmet odlučivanja. Kada se posmatra grafički, stablo odlučivanja je predstavljeno tako da grane stabla prikazuju moguće alternativne pravce, a [39]orovi mesta na kojima se donosi odluka. Stablo odlučivanja se formira na osnovu formiranja lanca međusobno povezanih i zavisnih odluka koje učestvuju u kreiranju i donošenju konačne poslovne odluke.

Osnovne k[5]mponente stabla odlučivanja su ciljna varijabla (koren) koja je u stvari celi uzorak, kao i čvorovi, grane i lišće. Stablo se grana za svaku vrednost testnog atributa, tako da se koraci ponavljaju rekurzivno sve dok se ne dostigne neki od kriterijuma koji zaustavlja rekurziju. Prilikom formiranja stabla odlučiva[43] važno je znati kako postaviti pravo pitanje. Modeli koji su zasnovani na stablima odlučivanja razlikuju se prema algoritmima koji zahtevaju karakteristike pojedinih podataka na osnovu kojih se kreiraju pitanja.

U teoriji, postoji eksponecijalno veliki broj [30] stabla odlučivanja koja se mogu formirati od nekog niza atributa. Neka stabla odlučivanja imaju veću preciznost od drugih, tako da je pronalaženje optimalnog stabla zbog eksponencijalne veličine prostora za pretraživanje računarski neisplativo. To je razlog zbog čega su razvijeni ef[63]sni algoritmi koji mogu indukovati precizno stablo odlučivanja u razumnom vremenu kao što su: *ID3*, *C4.5*, *CHAID*, *CR&T* i *QUEST*. Uglavnom, većina algoritama *koriste* metodu pretraživanja od vrha prema dnu (engl. *top-down*). [218]

Stablo odlučivanja spada u klasifikacione [5] metode rudarenja podataka, a prilikom analiza često se kombinuje sa metodom klasterovanja (engl. *Classification and Regression Trees*, *CART*). Zavisno od slučaja da li se koriste za predviđanje kategoričkih ili

kontinuiranih varijabli razlikujemo klasifikaciona stabla i regresiona stabla.

5.3.6 Metode za analizu veza (asocijativna pravila)

Metoda za analizu veza (asocijativna pravila) koristi se u obradi podataka u obliku transakcija. Osnovni zadatak u istraživanju podataka primenom asocijativnih pravila je pronalaženje međusobnih veza kojima se može opisati pojavljivanje pojedinih instanci (asocijacija) unutar velikih skupova podataka. Identifikovane veze se predstavljaju u formi $if - then$ pravila koja su zbog svoje jednostavnosti i razumljivosti koristan metod za predstavljanje znanja. Osnovna svrha algoritama za generisanje asocijativnih pravila je pronalaženje frekventnih skupova parova atribut-vrednost (engl. *frequent item sets*). Na početku vrši se formiranje podskupova koje čine po jedan elemenat atribut–vrednost, dok se u sledećim iteracijama povećava broj elemenata u skupovima. U svakoj sledećoj vrši se kreiranje podskupova od kombinacije samo elemenata frekventnih podskupova iz prethodne iteracije. Metrika pomoću koje se vrši zaključavanje frekventnost podskupa nazvana je podrška (engl. *support*). Konačan skup asocijativnih pravila određuje se korišćenjem metrike poverenja (engl. *confidence*).

Asocijativna pravila se predstavljaju u obliku $X \rightarrow Y$, pri čemu implikacija znači istovremeno događanje, a ne uzročnost. Implikacije asocijativnih pravila mogu se naći i sa leve i sa desne strane bilo koje kombinacije parova atribut–vrednost. Često se javlja slučaj generisanja pravila koja sa desne strane implikacije imaju uvek prikazanu informaciju o vrednosti samo jednog atributa. To su tzv. klasna asocijativna pravila (engl. *class asociation rules*), i tada se atribut čija se vrednost pokazuje naziva klasni atribut.

Generisanje asocijativnih pravila je iterativni proces koji se svodi na sledeću šemu:

- generisanje tablice frekvencija pojavljivanja pojedinačnih elemenata,
- generisanje tablice frekvencija pojavljivanja dva različita elementa i
- generisanje tablice frekvencija pojavljivanja tri različita elementa.

Asocijacijativna pravila su pogodna za analizu tzv. „potrošačke korpe" (engl. *market basket analysis*) u trasakcionim sistemima, primarno zbog jasnoće i iskorišćenosti dobijenih pravila. Na osnovu jasno izražene korelacije važnih proizvoda, sugerišu se konkretne akcije. Asocijativna pravila se primenjuju u obradi podataka kod kojih su atributi nominalnog (kategoričkog) tipa. Za proces primene ove tehnike važno je efikasno rešiti i probleme izbora pogodnog skupa elemenata i praktična ograničenja. Za skupove sa više elemenata (engl. *itemsets*) broj kombinacija raste eksponencijalno sa brojem elemenata u transakcijama.

Dobre strane metode asocijativnih pravila ogledaju se u jednostavnosti i jasnoći pravila. Ova metoda je namenjena problemima koji nisu klasifikacionog odnosno prediktivnog tipa. Isto tako, algoritmi kojima se generišu asocijativna pravila u principu su vrlo jednostavni. Asocijativna pravila 106liziraju međuzavisnost (frekvenciju veza) između svih atributa skupa koji su korisni za učenje, ukazujući koliko često se oni pojavljuju zajedno. Bilo koji atribut (ili skup atributa) može se koristiti za predviđanje vrednosti bilo kog drugog atributa.

5.3.7 Genetski algoritmi

Genetski algoritmi uglavnom se koriste kao tehnike za rešavanje problema optimizacije i predstavljaju heurističku metodu. U procesu rudarenje podataka oni se ne koriste za prepoznavanje uzoraka samih po sebi, ali se mogu uspešno primeniti pri kreiranju novih postupaka i metoda u samom procesu rudarenja. Funkcionisanje genetskih algoritama

uključuje nekoliko etapa:[220]

- pronalaženje genoma i fitness funkcije i kreiranje inicijalne generacije genoma,
- inicijalna modifikacija populacije kroz selekciju, *crossover* tehnike i mutaciju i
- ponavljanje prethodne etape sve dok se povećava prosečna vrednost *fitness* funkcije.

Selekcija u genetskim algoritmima obezbeđuje najjačim jedinkama prenos genetskog materijala na sledeće generacije, slično kao i u prirodi. U genetskim algoritmima se to odnosi na maksimum funkcije, odnosno genom koji utiče na najvišu vrednost *fitness* funkcije i on se utvrđuje kao najuspešniji. [220]

Genetski algoritam primenjuje koncept mutacije pravila ili obrazaca, koji su već identifikovani. Fokus kod genetskog algoritma je na pravilima, a ne na ulaznim podacima. Ulazni podaci se koriste da bi se testirala mutirana pravila. Kao izlaz genetskog algoritma nije predviđena zavisna promenljiva. Umesto toga, izlaz genetskog algoritma je pravilo koje može da predvidi zavisnu promenljivu. U određenoj formi genetski algoritam kombinuje dva pravila dajući novo pravilo koje deli karakateristike pravila roditelja. Zatim se vrši testiranje sposobnosti tog novog pravila da predvidi zavisne promenljive.U drugoj formi genetskog algoritma, dva pravila su stavljena jedno protiv drugog. Slabije pravilo se odbacuje, a jačem pravilu je dozvoljeno da nastavi sa malim slučajnim modifikacijama. Pravilo koje je rezultat ove metode se zatim testira za sposobnost predviđanja zavisne promenljive. [221]

Genetski algoritmi zasnivaju svoj rad na principu genetske modifikacije, mutacije i prirodne selekcije. U suštini oni stvaraju određen broj nasumičnih rešenja problema. Rešenja ne moraju biti efikasna. Može se javiti slučaj da je neka grupa rešenja preskočena, a može da dođe i do preklapanja rešenja. Dobra rešenja se se zadržavaju a loša odbacuju. Dobra rešenja se zatim hibridizuju i ceo proces se ponavlja. Slično procesu prirodne selekcije, na kraju ostaju samo najbolja rešenja. Najveći nedostatak ove metode je što zahteva ogromnu procesorsku snagu i što je prespora za trivijalne probleme. [221]

5.4 Korišćenje znanja otkrivenog u procesu rudarenja podataka

Kompanije kroz primenu rudarenja podataka vrše stvaraju upravljačke informacije dobijene iz podataka o poslovanju koji se nalaze na različitim transakcionim sistemima i koji dolaze iz različitih unutrašnjih ili spoljašnjih izvora. Alati za rudarenje podataka mogu se uvrstiti u alate poslovne inteligencije i pomoću njih se realizuje automatsko pretraživanje karakterističnih matrica ili korelacija između raspoloživih podataka. Koristeći podatke za donošenje efikasnh i pravovremenih poslovnih odluka možemo zaključiti da rudarenje podataka predstavlja i proces otkrivanja znanja. Prilikom korišćenja rudarenja podataka u svom poslovanju, kompanije omogućavaju sebi pored pristupa, analizu i korišćenje tih podataka kako bi ostvarile kvalitetno donošenje poslovnih odluka i upravljanje. Pored toga, tehnike rudarenja podataka omogućavaju kompanijama i postavljanje upita i dobijanje različitih izveštaja, realizaciju *on-line* analitičke i transakcione obrade podataka, kao i realizaciju statističkih analiza.[222]

Savremena praksa u poslovanju često podrazumeva analitiku podataka dobijenih iz različitih softverskih sistema, sa različitih računara i iz različitih baza podataka, tako da je to razlog za čvršćom integracijom različitih tehnologija podrške poslovnog odlučivanja u koje spada i rudarenje podataka. Nakon obavljenog postupka rudarenja podataka u kome se otkrivaju nizovi korisnih pravila, a u svrhu uspešne upotrebe i interpretacije pravila, potrebno ih je povezati i formalizovati.

U opštem slučaju, rudarenje podataka je primenjivo u svim područjima gde se raspolaže sa velikom količinom podataka. Iz domena područja određenog interesovanja kompanije i na osnovu otkrivenih podataka mogu se otkriti određene pravilnosti, veze i zakonitosti što je opet dobra primena rudarenja podataka. Imajući u vidu da postoji čitav niz faktora koji mogu uticati na ishod nekog događaja, zadatak rudarenja podataka je da identifikuje najvažnije faktore i njihove karakteristike u odnosu na ciljana stanja. Drugim rečima, bez obzira na područje primene, dobro iskorišćene metode rudarenja podataka mogu da otkriju zakonitosti iz velike količine podataka, pri čemu sada područje primene dolazi u drugi plan.

Snaga primene ove metode je u činjenici da je rudarenje podataka nezavisno od područja gde se primenjuje, jer se akcenat stavlja na podatke, a ne na područje u kome se realizuje analiza. Uspešnost primene metoda i alata rudarenja podataka zavisinajviše od stručnosti i poslovne kompetenciji lica koja procenjuju rezultate.

5.5 Područja za primenu alata za rudarenje podataka

Sagledavajući primenu rudarenja podataka možemo konstatovati da je cilj njegove primene otkrivanje nepoznatih karakteristika podataka, nepoznatih veza, zavisnosti ili tendencija, pri donošenju poslovnih odluka u kompaniji. Rudarenje podataka predstavlja relativno novi alat za podršku odlučivanju u kompaniji, koji analizira operativne podatke, otkriva probleme ili mogućnosti, formira računarske modele, zasnovane na tim otkrićima i koristi te modele za predviđanje u budućnosti.

Kratkoročno gledano, najveća primena rudarenja podataka vezana je za povećanje profita u kompanijama. Sama primena rudarenja podataka najkorisnija je tamo gde je realno prisutna velika količina podataka. [222] Na osnovu informacija dobijenih nakon rudarenja podataka može se lakše doći do saznanja o načinima za rešavanje ili smanjivanje problema koji se pojave u kompanijama. Akademski krugovi pretpostavljaju da će rudarenje podataka biti integrisano u potpunosti u svakodnevicu što će širokoj grupi korisnika ova tehnologija omogućiti da planira skoro svaki segment ličnog i poslovnog života.

Pravilno integrisano skladište podataka i dobro poznavanje i razumevanje procesa poslovanja nad kojim se želi primeniti postupak rudarenja podataka od presudne su važnosti za uspešno rudarenje podataka. Osim toga, za primenu rudarenja podataka potrebno je veliko statističko predznanje, a u praksi kompanije obično imaju mali broj analitičara koji se time bave. Procesom rudarenja podataka ne mogu se rešiti svi problemi koji se stavljaju ispred kompanija i njenih menadžera. Metode rudarenja podataka nisu univerzalne pa kompanije ne treba svu pažnju da usmeravaju na razvijanje novih algoritama i softvera, bez povezivanja sa stvarnim problemima sa kojima se suočavaju. Upravo je to razlog zbog koga je potrebno upoznati se sa primenom koncepta rudarenja podataka. S druge strane, ne treba imati nerealna očekivanja. U cilju izbegavanja nerealnih očekivanja, mora se imati u vidu da rudarenje podataka nije alat za definisanje problema ili otkrivanje šansi na tržištu. Ono samo pomaže u identifikaciji obrazaca u podacima, novih saznanja, koja će pomoći menadžerima kompanija u poslovnom odlučivanju, nakon utvrđivanja problema ili perspektiva koje treba iskoristiti. Sama primena rudarenja podataka, kroz bolje upravljanje i analizu podataka, može pomoći kompanijama da ostvare veće ili željene profite.

Bez obzira na velike mogućnosti, tehnologije rudarenja podataka nose i potencijalne opasnosti za kompanije. Najveća opasnost koja vreba je pitanje privatnosti.

Ovo je realan problem pošto je već ranije u radu konstatovano da su baze podataka sve veće i da je podat51 sve više. Kada svaki račun sa listom kupljenih artikala koji napravi lice ili kompanija uđe u bazu, ili kada su u bazi zabeleženi svi tele51ski razgovori lica u kompaniji, kada računar zabeleži svaku posećenu Internet lokaciju, kada svaka poseta lica lekaru i svaka bolest bude zabeležena u elektronskim kartonima, onda se sve što je u vezi sa bilo kojojm osobom stavlja na raspolaganje velikom broju zainteresovanih. Na prvi pogled je to gomila beznačajnih podataka vezanih za veliki broj zaposlenih u kompaniji ili stanovnika nekog grada ili države, to ne predstavlja problem specijalizovanim alatima koji se koriste za pretraživanje.

6. Memorija organizacije

Kompanije stvaraju informacije i znanje. Integracija znanja postaje ključni faktor uspeha svake kompanije. Sve veća složenost proizvoda, globalizacija, velika prisutnost na *Web*, društvene mreže, virtuelne organizacije, elektronsko poslovanje, usmerenost prema korisnicima, digitalne kompanije i razvoj Interneta/Intraneta zahtevaju sveobuhvatnu i sistematsku integraciju znanja unutar svake kompanije. [223] Rešenja se grade u okviru sistema integracije znanja. [224] Prilikom realizacije menadžmenta znanja kompanije su prinuđene da izvrše analizu i reše problem skladištenja i ponovnog korišćenja znanja na osnovu zahtevanih okolnosti. Kako bi olakšale korišćenje znanja i informacija, kompanije grade i koriste memoriju organizacije. Sistemi memorije organizacije pružaju procese za pronalaženje, pretraživanje i zahvatanje znanja i informacija.

Sam izraz memorija organizacije značajan je iz više razloga. Centralizovano upravljanje znanjem u kompaniji kao cilj ispred sebe uvek pretpostavlja ponovnu upotrebu eksplicitnih informacija, prećutnog znanja ili naučenih lekcija. Intuitivno, ponovna upotreba prethodno naučenih lekcija kroz skladištenje informacija (memorija organizacije), od ključnog je značaja za uspeh modernih kompanija. [225] U ovoj tački rada želimo da ispitamo memoriju organizacije kako bismo pronašli odgovarajuće osnovne teorijske konstrukcije. Naša namera nije stvaranje tehnoloških sistema memorije organizcije, već ispitivanje i razumevanje mesta memorija organizacije unutar okruženja kompanije.

6.1 Definicija memorije organizacije

Memoriju organizacije možemo posmatrati konkretno ili apstraktno. Ona se sastoji od nestruktuiranih koncepata i informacija koje postoje u organizacionoj kulturi i umovima zaposlenih u kompaniji, a koji se mogu delimično prikazati konkretnim memorijskim oblicima kao što su baze podataka. Takođe, memorija organizacije se sastoji od strukturiranih koncepata i informacija koje se mogu tačno predstaviti računarskim zapisima i datotekama. Memorija organizacije može se opisati u dva oblika kroz realizaciju dve funkcije: reprezentacije i interpretacije.

Tabela 14. *Forme i funkcije memorije organizacije*
Izvor: [228]

	Reprezentativne funkcije	Funkcije interpretacije
Konkretna forma	podaci dokumenta i *hypertext* formalizovano znanje formalizovana ekspertiza okruženje informacije	smernice za organizacione uređaje standardne operativne procedure
Abstraktna forma	kognitivne mape konceptualna sočiva okruženje	kultura ekologija jezik socijalna struktura

Kao ulazna tačka za razmatranje menadžmenta znanja unutar neke kompanije, u literaturi postoje više različitih i ponekad konkurentnih definicija memorije organizacije. Većina definicija memorije organizacije u dosadašnjoj literaturi počivaju na empirijskim pregledima u kontekstu njene upotrebe. Alvarado tvrdi da je memorija organizacije (organizaciona memorija engl. *organizational memory*) mesto kom mogu pristupiti

pojedinci radi učenja, podrške i donošenja odluka, razumevanja konteksta ili pronalaženja iskustva i stručnosti iz podataka, informacija i znanja kompanije. [226] Garcia i Howard memoriju organizacije predstavljaju kao kombinaciju baze znanja, objekata i ljudi, koji su u neprekidnoj i neraskidivoj interakciji. [227] Za Walsh i Ugsona memorija organizacije predstavlja istorijski zapis organizacije, koji se može preuzeti kako bi se podržalo trenutno donošenje odluka. [228]

U sagledavanju šta je to memorija organizacije korišćeno je puno pristupa u određivanju kako termina, tako i samog postojanja i shvatanja njene uloge u kompanijama. Heist i ostali kažu da memorija organizacije predstavlja *eksplicitno, odvojivo znanje, sačuvanu reprezentacija znanja i informacija u organizaciji*. [229] Huang i ostali i Euzenat memoriju organizacije vide kao *skladište znanja i znanja pojedinaca koji rade na određenim poslovima*. [230][231] Iako postoje različiti stavovi u određivanju memorije organizacije, obično se memorija organizacije smatra važnim intelektualnim kapitalom za podršku kompanijama, koji može doprineti performansama organizacije i koji bi mogao da se čuva u memoriji organizacije. [229] Prasad i Plaza, definišu memoriju organizacije kao *kolektivne podatke i resurse znanja kompanija koja uključuju iskustva stečena na projektima, ekspetizama za reševanje problema, motive konkretnog dizajna i sl.* [231] Memorija organizacije može uključivati baze podataka, elektronska dokumenta, izveštaje, specifikaciju proizvoda, motive konkretnog dizajna itd. U svojim istraživanjima Pomian, tvrdi da se izgradnja memorije organizacije oslanja na *volji za očuvanjem znanja, kako bi se znanje najbrže ponovo koristilo kasnije, kroz rasuđivanje, ponašanje, znanje čak i u njegovim suprotnostima i svim njegovim varijantama*. [232] Simon tvrdi da je *iskorišćavanje znanja proces koji omogućava da se na odgovarajući način ponovo upotrebi znanje o datom domenu, ranije uskladištenom ili modeliranom, kako bi se izvršili novi zadaci*. [234] Grundstein, razmatrajući memoriju organizacije rekao je da *svrha da se otkrije i objavi znanje kompanije, da kompanija bude u stanju da zadrži znanje, pristupi znanju i aktuelizuje ga, da kompanija zna kako da široko primeni to znanje i kako da ga bolje iskoristi, odnosno da ga podredi cilju i odredi njegovu pravu vrednost*. [235]

U poboljšanju svoje konkurentnosti memorija organizacije igra ključnu ulogu za korporacije u poslovanju. Čonsek kaže da je memorija organizacije važna jer predstavlja skup prakse koje su naučene kroz duži vremenski period, ponekad na teži način, i to svakoj kompaniji daje posebnu prednost koja je čini konkurentnijom na tržištu[236].

Razne studije koje su obrađivale memoriju organizacije predložile su različite ideje i korišćene su u različitim područjima. Jussupova-Mariethoz i Probst [237] razvili su rešenje memorije organizacije kao segment vođenja kompanije u sticanju, merenju, praćenju i upravljanju intelektualnim kapitalom. Od strane Stein i Zwass [238] predloženo je rešenje memorije organizacije podržane informacionom tehnologijom kao aktivnost koja dovodi do produktivnosti kompanije. Huang i Tseng [239] predložili su nove načine razvoja memorije organizacije pomoću korišćenja proširivog jezika oznaka (*XML*) koji je usmeren na produktivnije istraživanje korisnih znanja rudarenjem *Web*. Azbel i Berman [240] predstavili su novi model koji kombinuje ideje iz strukture memorije organizacije sa konceptima iz epistemiologije kako bi se uvela sredstva modelovanja znanja o grupama.Verma, Tiwari, i Mishra [241] predstavili su svoj koncept shvatanja memorije organizacije kao potrebna znanja koja se čuvaju u memoriji skladišta podataka kompanije za njegovu sadašnju i buduću upotrebu u *on-line* poslovanju. Ceusters i Smith [242], su stava da su za izgradnju robusnih i korisnih memorija organizacije, potrebne ontologije zasnovane na realnosti (određivanje opšteg) u kombinaciji sa referentnim praćenjem (određivanje specifičnog) što može imati odlučujuću ulogu za oslobađanje korporacija od tradicionalnih barijera koje nameće menadžment znanja. Mendenhall [243] je u svojim

tvrdnjama naveo da memorija organizacije doprinosi integrisnom sistemu dizajniranja i analize u vazduhoplovnoj industriji, naročito u situacijama kada inženjeri odlaze u penziju ili napuste kompaniju. Kühn and Abecker [244] predložili su opšti okvir za metodologiju razvoja, arhitekturu i tehničku realizaciju memorije organizacije koja se može okarakterisati kao sveobuhvatni računarski sistem.

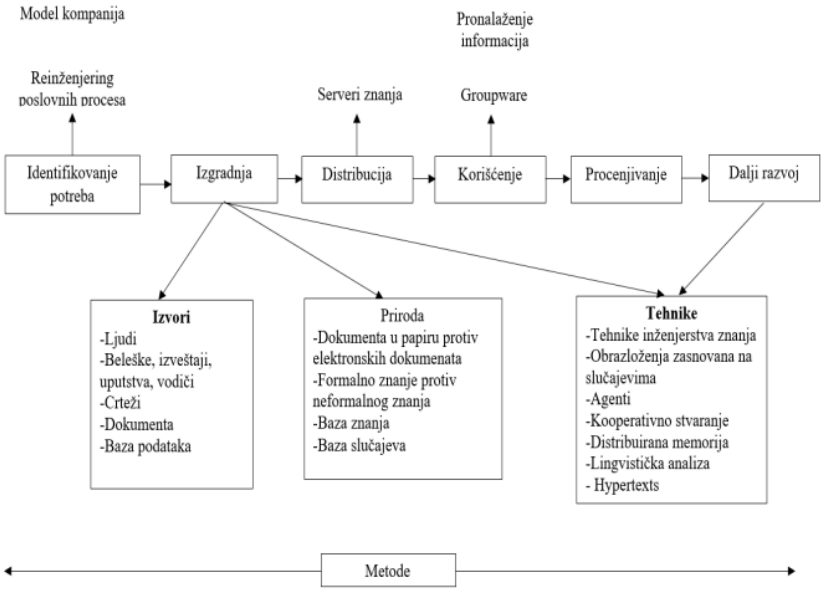
Iako se pojam memorija pojavljuje u organizacijskom smislu svuda u kompaniji; ipak, termin je ograničen na samo nekoliko područja primene. Ipak, teorijski koncepti memorije organizacije, doživele su puno izmena. Sam pojam memorije organizacije nepotrebno je ograničen samo na njenih nekoliko primena usmerenih na određene tehnologije. Ipak, nemoguće je sagledati memoriju organizacije kao samostalni činilac jer se ona pojavljuje u svim delovima organizacije.

6.2 Upravljanje memorijom organizacije

U kompanijama se danas može naći na dve vrste znanja: eksplicitno ili tacitno znanje[46]. To je razlog zbog koga je u bilo kojoj operaciji kapitalizacije znanja veoma važno izvršiti identifikaciju ključnog znanja čija se kapitalizacija zahteva. [245] To utiče na izbor vrste memorije organizacije koja je potrebna kompaniji. Memorija organizacije treba da pomogne u integraciji resursa i znanja u kompaniji i doprinese produktivnoj saradnji između aktivne dokumentacije i komunikacije sa skladištem podataka. [246] Prilikom razmatranja memorije organizacije u prvi plan se ističe pravovremeno obezbeđivanje potrebnog znanja ili informacije odgovornom licu na odgovarajućem nivou.

Kao što je utvrđeno u [42][247], lanac znanja se sastoji od sedam segmenata: navođenje postojećeg znanja, utvrđivanje potrebnog znanja, razvijanje novih znanja, dodeljivanje novih i postojećih znanja, primena znanja, održavanje znanja i odlaganje znanja. Sagledavajući ovu tvrdnju možemo prihvatiti proširenu definiciju memorije organizacije koju su predložili Van Heijst, Van der Spek i Kruizing, [229] *kao eksplicitno, bezobličnо trajno predstavljanje znanja i informacija u organizaciji, kako bi mu se olakšao pristup i omogućila ponovna upotreba od strane odgovarajućih lica iz organizacije u izvršavanju njihovih zadataka*. U tom kontekstu Dieng i saradnici [248] predlažu razmatranje izgradnje memorije organizacije kroz oslanjanje na sledeće korake: otkrivanje potreba u memoriji organizacije, izgradnja, difuzija, korišćenje, evaluacija, održavanje i razvoj memorije organizacije.

Za svaki korak izvršićemo analizu nekih metodoloških ili tehničkih predloga koje nude istraživači. Potrebno je napomenuti da kada je u pitanju navedena tematika postoji nekoliko vrsta publikacija koje se koriste u navedenom metodološkom pristupu: ankete o memoriji organizacije, analize vrste znanja dostupnih u kompanijama, izveštaji o industrijskim eksperimentima, predlozi opšte arhitekture za memoriju organizacije, detaljna studija tehnike obrade znanja koja proizilazi iz veštačke inteligencije, a u ovim slučajevima koriste se za reševanje specifičnih problema koji se nalaze u osnovi izgradnje memorije organizacije.



Slika 30. *Upravljanje memorijom organizacije*
Izvor: [249]

Jasno je da ovakav složeni problem sadrži nekoliko organizacionih i tehničkih aspekata čije je rešenje potrebno. Prema trvrdnjama Kühna i Abeckera [244] računarski naučnici koji se bave upotrebom informacionih i komunikacionih tehnologija za podršku memorije organizacije često imaju tendenciju da ignorišu specifične zahteve i ograničenja u industrijskoj praksi za uspešan menadžment znanja, dok eksperti koji se bave samom memorijom organizacije često samo približno tretiraju aspekte računarske podrške.

Kompanija nije samo jedinica proizvodnje robe ili usluga u skladu sa očekivanjima klijenata, u najboljim uslovima troškova, roka, kvaliteta, već naprotiv, kompanija je i jedinica za prozvodnju znanja tvrdi Grundstein [235]. Priroda potrebne memorije organizacije i potrebni napori za njenu izgradnju mogu zavisiti od veličine kompanije. Motivi za izgradnju memorije organizacije su različiti:

- izbegavanje gubitka znanja nekog eksperta nakon njegovog penzionisanja ili odlaska iz kompanije,
- iskorišćavanje iskustva stečenog na ranijim projektima (naučiti lekcije iz prošlosti kako bi se izbegla reprodukcija neke greške),
- iskorišćavanje mape znanja kompanije za korporativnu strategiju,
- poboljšavanje cirkulacije informacija i komunikacije u kompaniji,
- poboljšavanje učenja zaposlenih u kompaniji,
- integrisanje različitih znanja i iskustava kompanije.

Memoriju organizacije predstavljaju informacije koje neka kompanija stvara, i za koje se smatra da su vredne kako bi se ponovo koristile. Samim tim, javlja se potreba za novim zanimanjem u budućnosti – menadžer korporativne memorije.

6.3 Tipologija memorije organizacije

U literaturi koja obrađuje oblast memorije organizacije predloženo je nekoliko tipologija znanja u kompaniji.Ove tipologije prema tvrdnjamaDurstewitzamogu biti korisne za određivanje osnovnih znanja koje kompanija treba da kapitalizuje. [246] Sa jedne strane Grundstein i Barthès, [235][245] razlikuju *know-how* sposobnost, a sa druge individualne i kolektivne veštine. Oni razlikuju materijalne elemente kao što su podaci, postupci, planovi, modeli, algoritmi, dokumenta analize i sinteze, kao i nematerijalne elemente kao što su sposobnosti, profesionalne veštine, lično znanje, poznavanje prošlosti kompanije i konteksta odlučivanja u kompaniji. To je razlog zbog čega Grundstein i Barthès, [235][245] predlažu da se prilikom operacije kapitalizacije znanja kroz memoriju organizacije mogu uzeti u obzir materijalni elementi, dok nematerijalni elementi zahtevaju fomralizaciju znanja. Durstewitzdalje tvrdi da su primeri tipova znanja korisnih za memoriju organizacije: *know-how*, tehničke činjenice, zahtevi proizvoda, obrazloženje, iskustvo ili stručnost. [246]

Prilikom razmatranja tipologija memorije organizacije postoje nekoliko razmišljanja. Pomian, [233] tvrdi da memorija jedne kompanije obuhvata ne samo tehničku memoriju dobijenu kapitalizacijom znanja svojih zaposlenih, već i organizacionu memoriju (ili menadžersku memoriju) koja se odnosi na prošlu i sadašnju organizacionu strukturu kompanije (ljudski reusursi, upravljanje itd.) i memoriju projekata za kapitalizaciju lekcija i iskustava iz datih projekata. Tourtier, [250] razlikuje nekoliko vrsta memorije:

- memoriju profesije – sastavljenu od refernci, dokumenata, alata, metoda koji se koriste u određenoj profesiji;
- memoriju kompanije – koja je vezana za organizaciju, aktivnosti, proizvode, učesnike (npr. kupci, dobavljači ...);
- individualnu memoriju – koju karakteriše status, kompetencije, *know-how*, aktivnosti određenog člana kompanije;
- memoriju projekata – koja uključuje definiciju projekta, aktivnosti, istoriju i rezultate.

Grundstein i Barthès [245] razlikuju tehničko znanje kompanije (znanje koje se koristi svakog dana u kompaniji, od strane zaposlenih za realizaciju njihovih svakodnevnih aktivnosti) i streteško korporativno znanje koje koriste menadžeri kompanije.

Osim navedenih tipologija, potrebno je pomenuti i razliku između unutrašnje memorije (koja vrši korespodenciju sa znanjem i informacijama unutar kompanije) i spoljašnju memoriju (koja vrši korespodenciju sa znanjem i informacijama van kompanije, koje potiču iz spoljašnjeg sveta).

6.4 Informatičke pretpostavke za formiranje memorije organizacije

Kao i kada je u pitanju uspešan razvoj informacionog sistema uopšte, tako i uspešan razvoj memorije organizacije kao sistema mora biti usmeren jasnim fokusom na situacije korišćenja i potrebe korisnika. [251] Buckingham tvrdi da je istorija razvoja sistema pokazala da su ljudska pitanja ta koja stvaraju ili brišu nove metode i alate u poslovanju [252]. To je razlog zbog čega je prvi zadatak dizajnera memorije organizacije otkrivanje i identifikacija potreba korisnika, ili potreba memorije organizacije.

Otkrivanje i identifikacija potreba nije jednostavno. Dizajneri memorije organizacije moraju imati što više saznanja o tome ko su korisnici, koje zadatke korisnici trebaju da realizuju, u kojim situacijama, koje vrste znanja treba zapamtiti i preuzeti, koje alate će koristiti itd. Sve ovo dizajnere memorije organizacije suočava sa problemima koji su vezaniza korisnike, zadatke, situacije itd. Ti problemi su:

- Vrste korisnika – Potrebno je razmotriti: Ko su stvarni korisnici? Kako uzeti u obzir brojnost korisnika memorije organizacije? Da li je vredno razmišljati o svakom potencijalnom korisniku memorije organizacije? [253].
- Karakteristike i ponašanje korisnika – Koje su karakteristike i ponašanja stvarnih korisnika koje je potrebno razmotriti? Kako uzeti u obzir višestruke i verovantno neujednačene perspektive korisnika? [254] Možemo li da ignorišemo ponašanje posrednih korisnika kao poverenje? [255] Koji je značaj čuvanja i prikupljanja znanja prilikom aktivnosti korisnika tokom izvršavanja njihovih zadataka?
- Zadaci – Koji su stvarni zadaci ili ciljevi koje je potrebno razmotriti? [234] Ovo je potrebno u kontekstu razmatranja dinamičnih složenh situacija kroz identifikaciju određenih ciljeva memorije organizacije kao što su: inovativnost, povećanje saradnje, upravljanje preuzimanjem, postupanje sa izuzecima, suočavanje sa kritičnim situacijama.
- Situacije – Koje su stvarne situacije ili konteksti koje je potrebno razmotriti? Dinamički složene situacije kao što su: upravljanje u slučaju opanosti, kontrola saobraćaja, usluge spašavanja, industrijska kontrola postrojenja, podrazumevaju znatno drugačije zahteve za memoriju organizacije.
- Znanje – Koje je stvarno znanje koje je potrebno razmotriti? Gde se to znanje dobija? Šta možemo učiniti ako su korisnici izvora koji poseduju stvarno znanje premešteni, dali ostavku, otpušteni ili su penzionisani? [253]
- Greške – Koje su važne greške memorije organizacije koje je potrebno razmotriti? Kako se ponašati sa tim greškama? [256]

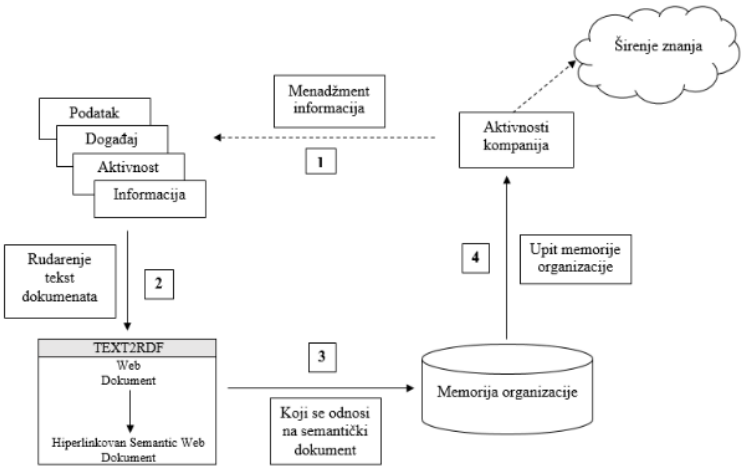
Dizajneri memorije organizacije u svom radu suočavaju se ne samo sa direktnim problemima sa korisnicima, već i sa problemima koji direktno utiču na dizajnera. Prilikom razmatranja problema koji direktno utiču na dizajnera, mora se uzeti u obzir činjenica da oni mogu imati velike implikacije prilikom rešavanja utvrđivanja i identifikacije potreba. To su sledeći problemi.

- Ambicije projekta memorije organizacije – Da li je projekat realan? [257].
- Perspektive dizajna memorije organizacije – Da li je cilj da se napravi potpuno novi dizajn memorije organizacije ili da se poboljša postojeći (izvrši redizajn)?
- Osnovno predstavljanje memorije organizacije – Da li se memorije organizacije posmatraju kao predmet (objekat) ili kao proces [258]?
- Paradoks produktivnosti – Kako se nositi sa paradoksom produktivnosti, pri čemu dostupnost sve više informacija zapravo uzrokuje smanjenje proizvodnje korisnika. [259]
- Paradoks konteksta – Kako se nositi sa mogućnošću potrebe šireg konteksta za proučavanje i razumevanje bilo kakvih kontekstualnih informacija. [252]

Postoje nekoliko usvojenih rešenja za otkrivanje i utvrđivanje potreba memorije

organizacije.

Osnovni pristup predstavlja *Stakeholder-Centered Design*. Iz osnovnog pristupa razvoja memorije organizacije nemoguće je isključiti pristup detektovanja potreba. On je zasnovan na centralno orijentisanom korisničkom dizajnu (engl. *User-Centered Design, UCD*), ili na pristupu ljudski centralno orijentisanog dizajna (engl. *Human-Centered Design, HCD*). Razlog korišćenja HCD je da bi se obezbedio uslov da se memorija organizacije definiše u smislu potreba korisnika [246]. Povezivanjem metoda UCD i HCD kroz razmatranje društvenih i tehničkih pitanja u novom razvoju sistema vrši se objedinjavanje određivanja, oblikovanja i implementacije zahteva.



Slika 31. *Okvir upravljanja memorijom organizacije*
Izvor: [260]

Sama filozofija na kojoj se zasniva ovakav pristup je stvaranje efiksanog sistema kroz partnerstvo između programera i korisnika i/ili zainteresovanih strana u kompaniji koja upravlja novim sistemom [261]. Ovde je potrebno razjasniti značenje termina *stakeholders* . Ovaj pojam se odnosi na „svakog pojedinca unutar neke grupe gde se može implementirati neki sistem koji ima interes na koji sistem može da utiče" [261], i on se odnosi na „bilo koga koji stiče neku dobit od tog sistema i onoga koji može izgubiti u pogledu tog sistema" [262].

Tradicionalni pristup predstavlja u stvari pristup struktuirane analize ili objektno orijentisani pristup. U ovom pristupu korisnici imaju pasivnu ulogu; gde se razmatraju kao izvori informacija i kao recenzenti razvijenih modela, dok je analitičar sistema odgovoran za traženje zahteva od korisnika. Od korisnika se očekuje da kroz analizu svojih potreba, razne upitnike, ankete i slično pruže pomoć i time daju svoj doprinos. U slučajevima kada inicijatori projekta nemaju sve potrebne informacije kako bi dizajnirale promene u samom sistemu, korisnici imaju mogućnost da ne prihvate to rešene u toku dizajniranja sistema. Preporuka je da se formira tim dizajnera kako bi se olakšala tranzicija od zahteva ka dizajnu. U timu dizajnera jasno su identifikovane uloge tehničkih eksperata i kupaca.

Pristupom grupnih sesija vrši se zajedničko dizajniranje sistema. Macaulay, [262] zagovara pristup koji je usmeren na zainteresovane strane i koji čine sledeći koraci: identifikacija problema, formulisanje tema, grupna sesija 1 (istraživanje korisničkog okruženja, validacija sa korisnicima), grupna sesija 2 (identifikacija obima predloženog sistema, validacija sa zainteresovanim stranama). Svaka grupna sesija ima niz koraka.

Svaki korak uključuje uvod, *brainstorming*, prioritizaciju i generisanje dogovorenih opisa koristeći kontrolne liste i forme koje se bave problemima vezanih za korisnike. Veoma je važno konstatovati da je analiza zahteva u velikoj meri povezana sa evaluacijom. Thomas tvrdi da ako je cilj analize zahteva usmeravanje ka potrebama korisnika, onda je cilj evaluacije da prilagodi sistem kako bi on zaista mogao da zadovolji potrebe korisnika. [251]

Klasične metode za otkrivanje potrebe memorije organizacije čine: pregled litarture, intervjui/diskusije i opservacije/eksperimenti. Pregled literature koristi se kako bi se otkrile potrebe memorije organizacije. Macintosh [263] to realizuje kroz menadžment imovinom znanja. Kühn i Abecker [244] identifikovali su sledeće glavne prepreke za veću produktivnost u procesima koji su zasnovani na menadžmentu i upotrebi znanja u kompanijama. Oni se se mogu razmatrati i kao uvod u zahteve:

- u procesu traženja potrebnih informacija visoko rangirani radnici u kompaniji troše veliki deo svog radnog vremena,
- esencijalne veštine znanja nalaze se samo u glavama nekoliko zaposlenih,
- vredne informacije nalaze se u gomilama dokumenata i podataka,
- greške koje puno koštaju kompaniju ponavljaju se jer se zanemaruju prethodna iskustva i
- kašnjenja i optimalan kvalitet prozvoda rezultat su nedovoljnog protoka infomacijna u kompanijama. [244]

Intervjui/diskusije koriste se za identifikaciju potreba memorije organizacije. Kako bi dobili potrebne zahteve Kühn i Abecker [244] realizovali su intervjue sa potencijalnim korisnicima, kao i diskusije sa IT licima i menadžerima u kompanijama. Oni za uspeh projekta memorije organizacije – informacionog sistema u industrijskom sektoru, predlažu sledeće ključne zahteve:

- prikupljanje, sistematizacija i organizacija informacija iz različitih izvora;
- integracija u postojeće radno okruženje;
- minimizacija inžinjeringa naprednog znanja;
- aktivno prikazivanje relevantnih informacija;
- korišćenje povratnih informacija korisnika za održavanje i razvoj sistema. [244]

Opservacije/eksperimenti služe za otkrivanje potreba memorije organizacije. Karsenty [264] je u svojim istraživanjima pokazao da manje iskusni dizajneri uvek izaberu rešenje memorije organizacije koje je razvio neki drugi, dok iskusni dizajneri razmatraju alternativna rešenja koja su spontano pronašli i dokazali da su uspešnija od ranijih rešenja. Ovi rezultati sugerišu zahteve da rešenja dizajnera memorije orgaizacije treba da sadrže opravdanje ili argumentaciono znanje za iskusne dizajnere koje je orijentisano na znanje iz prošlosti i znanje koje je orijentisano na sadašnje znanje za manje iskusne dizajnere. [264]

U razvoju memorije organizacije identifikovani su određeni trendovi. Urban i von Hippel[265] zagovaraju metodologiju vodećeg korisnika kroz otkrivanje potreba vodećih korisnika. Grundstein i Barthès [245], ponudili su svoje rešenje u obliku savetodavne analize za kapitalizaciju znanja (engl. *Advisibility Analysis for knowledge capitalization*) koja je orijentisana na procese i probleme. Ovaj pristup utvrđuje osetljive procese koji su od suštinske važnosti za funkcionisanje kompanije; razlikuje određene probleme koji čine

slabim kritične aktivnosti u kompaniji i određuje ključno znanje koje je neophodno za rešavanje problema. Određena istraživanja modela i pristupa u razvoju memorije organizacije koju je realizovao Fox fokusirana su na modelovanje kompanije. [266] Osnovni razmatrani elementi su: razvoj kompanije u jedinici vremena i iskustva stečena iz realizovanih projekata. Uschold, King, Moralee i Zorgios, tvrde, da je važna ontologija kompanije, kao i definisanje koncepata koji su relevantni za kompaniju. [267] Fraser tvrdi da ove ontologije mogu se koristiti kao podrška za razmenu informacija i znanja u kompaniji. [268] Modelovanje unutar kompanije ili modelovanje između nekoliko kompanija se razlikuju. Beauchène, Mahé i Rieu izvršili su modelovanje memorije organizacije, koristeći model koji proizilazi iz upravljanja kvalitetom i fokusira se na odnose između kupaca i dobavljača unutar kompanije. [269] Eksploatacija modela memorije organizacije predstavlja način određivanja slabih tačaka u kompaniji, a što bi u krajnjem slučaju dovelo do poboljšanja kapitalizacije znanja u kompaniji. Često se pravi razlika između proizvodno i procesno orijentisanih kompanija. Maurer i Dellen ponudili su proces modelovanja memorije organizacije za predstavljanje znanja na osnovu radnih procesa u kompaniji. [270] Feray i saradnici predložili su model memorije organizacije koji karakterišu elemenati: dokument, program, budžet, kontakti, kompanija, materijal, kalendar i rezultati. [271]

Kognitivni modeli baziraju se na kognitivnim funkcijama zaposlenih i korišćenje znanja u situacijama koje mogu biti korisne za otkrivanje potreba korisnika i kompanije u radnom procesu uopšte. U svojim istraživanjima Bollon je praktično pokazao svrsishodnost ovakvog modela, naročito metodoloških mera predostrožnosti koje se primenjuju tokom opservacije procesa u kompaniji kako bi se izvršila uspešna kapitalizacija znanja. [272] Wisneru svojim istraživanjima obrađuje pristup i metodologiju antropotehnologije koja se odnosi na transfer organizacionih sistema i tehnologija u državama sa različitim kulturama. [273] Identifikovan je još i model umrežavanja znanja (engl. *Knowledge Networking*). Sa stanovišta dizajnera memorije organizacije, projekat *CERES-GKN* predviđa događaje u budućnosti razvojne prakse memorije organizacije. Cilj ovog projekta razvoja memorije organizacije je izgradnja globalne mreže znanja koja će omogućiti ekološki zdrav razvoj proizvoda i procesa u kompanijama. Projekat će razviti i globalnu mežu baze znanja.

6.5 Stvaranje memorije organizacije

Memorija organizacije zahteva postojanost stečenog znanja svojih zaposlenih u kompaniji. Ovo se postiže zapisima iz iskustava zaposlenih, tokom izvršavanja njihovih poslovnih obaveza na različitim pozicijama u kompaniji. Sam dizajn memorije organizacije počinje, na osnovu podataka (kontekstualnih informacija), iz organizacionih pozicija u kompaniji. Znanja kompanije i iskustva potrebno je integrisati od individualnog znanja i iskustava zaposlenih u kompaniji. [274] Svaki zaposleni dok radi na nekoj poziciji u kompaniji, stiče iskustvo i vrši apstrahovanje znanja, tako kada takvo lice iz bilo kog razloga napusti svoj položaj ili kompaniju, dobit kompanije se ne gubi. Glavna dodatna vrednost memorije organizacije je upravo ta da znanje zaposlenih dok rade na svojim pozicijama u kompaniji, može biti strateški ponovljeno kao prednost te kompanije i u budućnosti.

Obično se svaka kompanija kroz integraciju zaposlenih u organizacione delove kompanije ili radne timove oslanja na neku strukturu. U skladu sa odgovornostima i uticajima ta struktura je hijerarhijski definisana. Svaki zaposleni zauzima određenu poziciju koja je profilisana u zavisnosti od njegovih sposobnosti i dodeljenih zadataka. To

je razlog zbog čega, svaki zaposleni realizuje specifične zadatke i istovremeno vrši akumulaciju srodnih iskustava. [161]

Memoriju organizacije možemo materijalizovati na dva načina kao neračunarski medijum i računarski medijum. Dieng i saradnici tvrde da prihvaćene tehnike za izgradnju memorije organizacije pre svega zavise od dostupnih izvora kao što su: eksperti, postojeća papirna ili elektronska dokumenta. Pored toga, tehnike zavise i od prirode potreba koje treba da ispuni memorija organizacije prema planiranim korisnicima. [248]. U svojim razmtranjima Simon kaže da memorija organizacije može biti i memorija koja je bazirana na informacionom sistemu koja se materijalizuje kroz inteligentne sisteme upravljanja dokumentima, bazama podataka, bazama znanja, sistema zasnovanih na studijama slučaja, sistema zasnovanih na *Web* tehnologijama ili multi-agent sistemima [234].

6.5.1 Nekompjuterizovana memorija organizacije

Neračunarska memorija organizacije sastoji se od znanja koje nije ranije korišćeno i koje se nalazi u dokumentima u papiru. Izgradnja ovakve vrste memorije organizacije može voditi ka dva različita cilja:

- elaboraciji sintetičkih dokumenata o znanju kompanije koje se ne nalazi eksplicitno u izveštajima ili tehnička dokumentacija koja se više odnosi na znanje i veštine stručnjaka kompanije i
- poboljšanju proizvodnje kompanije kroz predlog eksperata o svojim zadacima u procesu dizajna memorije organizacije.

Sagledavajući prvi cilj možemo zaključiti da se memorija organizacije sastoji od znanja opisanih u postojećim dokumentima i razgovorima sa ekspertima, odnosno, elaboracijom posmatranja aktivnosti u kompaniji od strane eksperata. [275] Simon, smatra da ovakva memorija organizacije pruža „globalni pogled na znanje kompanije" i „dozvoljava ekspertima sa različitih lokacija da opišu svoje znanje u istom formatu kako bi kasnije, mogli, da ih lakše upoređuju".[234] Ipak, ova elaboracija sinteze dokumenata prema Simonu predstavlja prvi korak u izgradnji računarske memorije organizacije koji pomaže u implementaciji znanja kompanije kroz omogućavanje homogenizacije znanja i veština na različitim geografskim lokacijama kompanije.

Posmatrajući drugi cilj, Corbel, koristeći iskustva kompanije *RENAULT* predložio je *MEREKS* pristup [276].Vođen je pristupom kvaliteta, i zasniva se na pozitivnom i negativnom povratku iskustva iz prethodnih projekata kompanije. Memorija organizacije sastoji se od obrasca, gde ekspert može opisati rešenje ili odluku u zadatku procesa dizajna. Ovi obrasci su validirani sistemom kontrolne liste i uskladišteni u sistemu upravljanja obrascima. Koriste se u fazi specifikacije proizvoda, koja prethodi dizajnu. [276]

6.5.2 Memorija organizacije bazirana na dokumentima

Memorija organizacije bazirana na dokumentima oslanja se na princip da svi postojeći dokumenti kompanije mogu činiti memoriju organizacije. Ipak, ta dokumenta nisu dobro indeksirana ili predstavljaju ličnu bibliografiju za svakog zaposlenog u kompaniji. Dakle, izgradnja jedne takve memorije organizacije započinje indeksiranjem svih izveštaja, sintezne dokumentacije ili referenci koje koriste različiti eksperti u kompaniji. Ovakva memorija organizacije zahteva okruženje za upravljanje dokumentima. Poitou, tvrdi da je dobar sistem zasnovan na dokumentaciji verovatno najjeftiniji i najizvodljivije rešenje za menadžment znanja, ali koje podrazumeva lice koje će biti zaduženo za vođenje takvog sistema. [277] Možemo konstatovati da u ovakvom sistemu dokument već vrši predstavljanje znanja kompanije. Ovde se javlja glavna potreba sistema

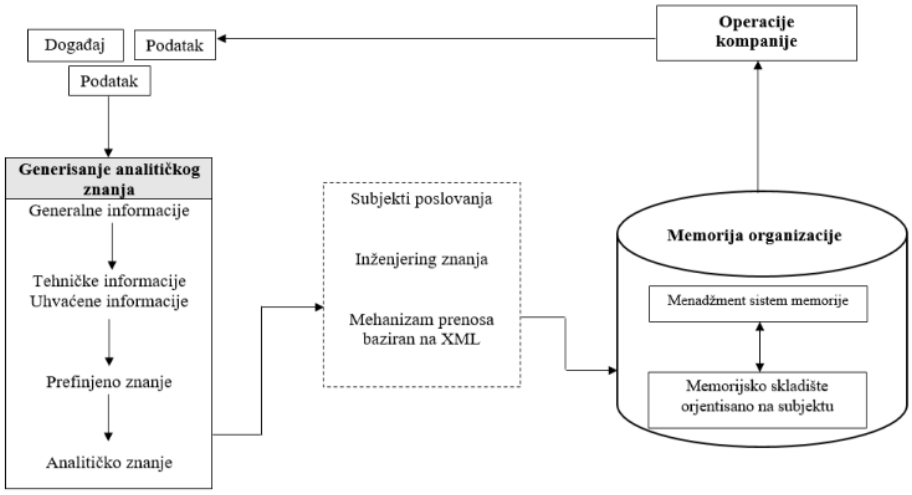
u smislu pomoći u pripremi, skladištenju, preuzimanju i obradi dokumenata kompanije. Poitou je u [277] predložio sistem kolektivnog upravljanja korporativnim znanjem, dok je od strane Ballay i Poitoua u [278] za ovakvu vrstu upotrebe razvijen predložen i predstavljen takav sistem.

Razrađujući svoj princip za menadžment znanja Ballay razlikuje nekoliko integracionih nivoa dokumenata čija se eksploatacija može realizovati u memoriji organizacije. [279] To su: kontrolne liste eksperata, vizuelni dokumenti, ikonografski dokumenti, uobičajeni kancelarijski dokumenti i multimedijalni – hiper dokumenti.

6.5.3 Memorija organizacije bazirana na menadžmentu znanja

Inženjerstvo znanja (engl. *knowledge engineering*) svojom svrhom korisno je za izgradnju memorije organizacije. Ovakva memorija organizacije zasnovana je na izjašnjavanju i eksplicitnom modelovanju znanja od strane eksperata, ili čak i od formalne predstave znanja koje u osnovi predstavlja dokument. To je razlog evolucije određenih ekspertnih sistema koji se koriste u izgradnji memorije organizacije kroz korišćenje iskustva iz prošlosti. Ipak, sam cilj izgradnje memorije organizacije manje je ambiciozan u poređenju sa ekspertnim sistemom. Umesto da cilj bude automatsko rešenja zadataka (sa automatskim mogućnostima razmišljanja) kao što je slučaj u ekspertnim sistemima, memorija organizacije treba da pomaže korisniku, gde će korisniku pružiti odgovarajuće korporativne informacije, uz odgovornost korisnika za kontekstualno tumačenje i procenu ovih informacija koje se nalaze u memoriji organizacije.

U svojim istraživanjima Kuhn i Abecker [244] primetili su da „u suprotnosti sa ekspertnim sistemima, cilj memorije organizacije nije podrška određenog zadatka, već bolja eksploatacija esencijalnog korporativnog resursa kompanije – znanja". Međutim, potrebno je napomenuti i da su neke memorije organizacije koje su zasnovane na znanju u praksi implementirane kao ekspertni sistem. O'Leari, [280][281] opisuje nekoliko vrsta baza znanja koje su korisne u konsultantskim firmama: baze znanja o angažovanju, baze znanja za predloge, baze znanja o vestima, baze znanja najbolje prakse, ekspertske baze znanja.



Slika 32. *Veza između analitičkog znanja i memorije organizacije*
Izvor: [239]

Metode za inženjering znanja kao što su *COMMET* i *CommonKADS* mogu biti korisne u izgradnji memorije organizacije, jer omogućavaju analizu i predstavljanje aktivnosti kompanije na nivou znanja. [282] Steels [283] primećuje da je organizacija proizvodnje u kompanijama sve više horizontalna, tj. proizvodnja u kompanijama organizuje se kroz aktivnosti grupisanja eksperata iz različitih delova kompanije. Dakle, memorija organizacije ovakve kompanije može biti zasnovana na opisu aktivnosti kroz tri perspektive: zadatak, metod i informacije. Na isti način, neki modeli koje nudi *CommonKADS* (organizacija, zadatak, agent, komunikacija i modeli ekspertize) daju zanimljivu osnovu za *memoriju organizacije koja je zasnovana na znanju*. [284][285][286]

Tabela 15. *Modeli CommonKADS i tipovi memorije organizacije*
Izvor: [287]

Tipovi memorije organizacije	**Relevantni CommonKADS modeli**
Profesionalna memorija	Ekspertni model (naročito modeli ontologije i modeli domena)
Memorija kompanije	Organizacija, zadatak, agent modeli
Individualna memorija	Agent, ekspertni modeli
Projektna memorija	Zadatak, agent, komunikacioni modeli
Tehnička memorija	Zadatak, agent, ekspertni modeli
Menadžerska memorija	Organizacija, zadatak modeli

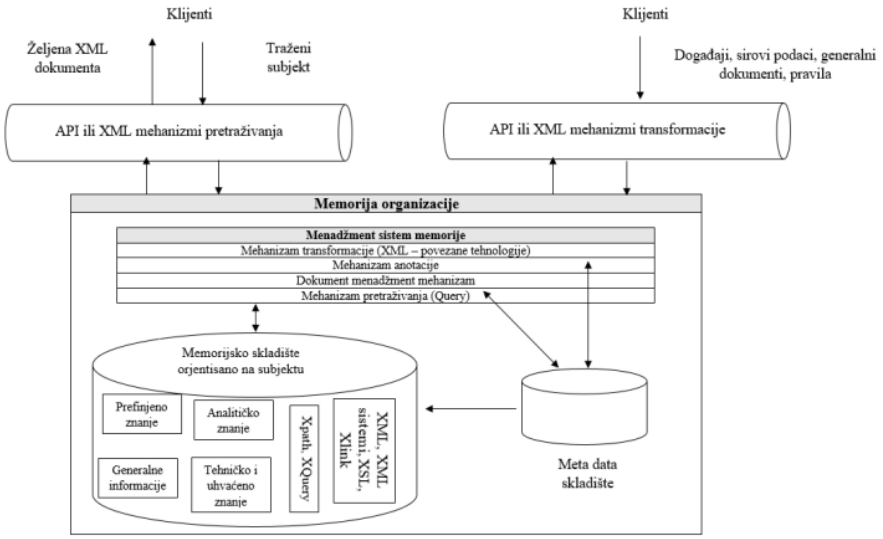
Za izgradnju memorije organizacije zasnovane na znanju mogu se koristiti i ontologije. Ontologije su korisne u memoriji profesije ili u tehničkoj memoriji, za predstavljanje terminologije i konceptualizaciju koju deli određena profesija u nekoj kompaniji. U svojim istraživanjima to je primetio O'Leary [281], koji tvrdi da *ontologije pružaju određenu strukturu za razvoj baza znanja, kao i osnovu za generisanje tačke gledišta na osnovu znanja*. Zbog toga, neke kompanije grade svoje ontologije u cilju izgradnje memorije organizacije zasnovane na znanju. Abecker, Bernardi, Hinkelmann i ostali [288], predložili su nekoliko vrsta ontologija koje nude „inteligentnu podršku prema kontekstno osetljivim saznanjima o znanju". To su: ontologija informacija (za strukturu, pristup i oblikovanje karakteristika izvora informacija); ontologija domena (za modelovanje sadržaja izvora informacija) i ontologija kompanije (za opis konteksta informacija u pogledu organizacione strukture i modela procesa u kompaniji). Istraživanje metoda ili alata za izgradnju novih ontologija, za ponovnu upotrebu već postojeći ili za njihovu vizuelizaciju obrađeni su u [289][290].

6.5.4 Memorija organizacije zasnovana na slučajevima

Korišćenje tehnika veštačke inteligencije, zasnovanih na slučajevima, može biti korisno za izgradnju memorije organizacije. [291][234] Svaka kompanija ima kolekciju prošlih iskustava (uspeha ili neuspeha) koje se mogu eksplicitno predstaviti u istom reprezentativnom formalizmu omogućavajući njihovo poređenje. Upotreba kolekcije slučajeva za predstavljanje memorije organizacije namenjena je: izbegavanju rasipanja ekspertize kroz koncentraciju znanja svih eksperata u pridruženim slučajevima i omogućavanju kontinuiranog razvoja memorije organizacije zahvaljujući progresivnom dodavanju novih slučajeva.

Razmišljanje zasnovano na slučajevima omogućava razumevanje koje je proisteklo iz iskustava, ali i slučajeva sa kojima su se u kompaniji već sretali, kako bi rešili nove probleme. Pronalaženje sličnog slučaja iz prošlosti može pomoći ekspertima u kompaniji za sugerisanje rešenja za novi problem koji zahteva rešavanje. Poboljšanje predstavljanja i ekspertize slučajeva, organizacije i indeksiranja osnovnih slučajeva, veoma je važno za povećanje efikasnosti prikupljanja povratnih informacija i efikasnosti rešavanja novih

problema u kompaniji. [292][293]



Slika 33. *Arhitektura i mehanizam pretraživanja memorije organizacije*
Izvor: [239]

Simon u [234] opisuje primer u metalurgiji, gde je cilj bio iskoristiti znanje i veštine iz opisa proizvedenih čeličnih i metalurških defekata i problema tokom proizvodnje. Ova metoda sastoji se od: stvaranja sintetičkih dokumenata zajedničkih za sve lokacije i poštovanja homogenog formata; predlaganja modela za implementaciju memorije organizacije na osnovu takve sinteze dokumenata; obezbeđivanje procesa kapitalizacije znanja koji omogućavaju korišćenje memorije organizacije u svrhu detekcije defekata. [234]

6.5.5 Izgradnja distribuirane memorije organizacije

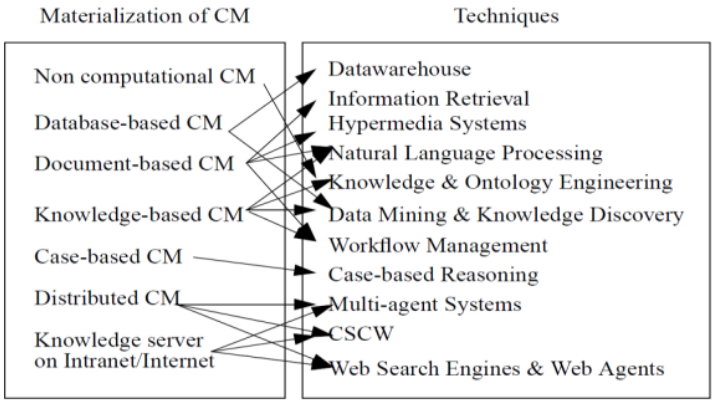
Distribuirana memorija organizacije interesantna je za podršku saradnje i razmene znanja između nekoliko grupa ljudi u kompaniji ili u nekoliko kompanija u korporaciji. Distribuirana memorija neophodna je za virtuelne kompanije koje su formirane od distribuiranih kompanija i timova ljudi koji se sastaju i rade zajedno *on-line*. Generalno, za takve virtualne kompanije distribuirana memorija prirodno se oslanja na eksploataciji Interneta i *Web*. [280] Možemo navesti primer, projekta inteligentne proizvodnje *GNOSIS* [294] koji uključuje nekoliko kompanija distribuiranih na nekoliko kontinenata. Koordinacija ovog projekta i upravljanja distribuiranog znanja između učesnika vrši se preko *Web*, dok se razvijeni alati u projektu koriste za održavanje memorije projekata korporacije. Drugi pristup, zastupaju Ribière i Matta, [295] i predlažu vodič za izgradnju memorije projekta sa više tački gledišta, u okviru virtualne kompanije čiji je sastav dizajnera iz različitih kompanija, a koji istovremeno sarađuju na inženjeringu projekta.

Distribuirana memorija organizacije može biti formirana od distribuiranih, heterogenih baza znanja ili distribuirane, heterogene baze slučajeva ili *multi-agens* sistema. Kao primer može poslužiti projekat *MEMOLAB* [296]. Nagendra, Prasad i Plaza tvrde da implementacija distribuirane memorije, takođe, može da se osloni i na distribuirane slučajeve biblioteka i na veštačke agente odgovorne za pronalaženje informacija između takvih biblioteka [232].

U izgradnji distribuirane memorije organizacije često su uključeni eksperti iz različitih oblasti. Protokol za kolektivno izražavanje znanja predložio je Dieng sa saradnicima u [248]. Problemi konzistentnosti dobijenih elemenata memorije organizacije kohabitacije nekoliko tačaka gledišta koje se moraju rešavati kroz protokol za kooperativno stvaranje konsenzualne memorije organizacije predstavio je Euzenat u [231]. U konkretnim slučajevima distribuirane memorije organizacije koji se oslanjaju na ponovnu upotrebu ontologija, istraživanju o saradnji stvaranja ontologija preko njihovog servisa mogu se koristiti *Ontolingua* [289], *APECKS* [290] ili *WebOnto* [297].

6.5.6 Kombinacija tehnika u izgradnji memorije organizacije

Kada to slučajevi zahtevaju kompanijama su potrebne obe vrste znanja – neformalno i formalno znanje (eksplicitno znanje predstavljeno u bazi znanja). To je razlog zbog koga se istraživanje na upravljanju vezama između dokumenta i baze znanja može koristiti kada je u pitanju memorija organizacije. [298][231] Na isti način, Trigano tvrdi da istraživanje poluautomatske ekstrakcije znanja iz dokumenata zahvaljujući prirodnoj analizi jezika takođe, može biti korisno. [299] U svojim istraživanjima Kuhn i Abecker i Abecker, Bernardi i ostali predlažu arhitekturu memorije organizacije gde se memorija organizacije može sastojati od različitih vrsta sećanja: dokumenata, baza podataka, znanja baze itd. [244][288]



Slika 34. *Veza između materijalizacije memorije organizacije i mogućih tehnika*
Izvor: [300]

6.6 Korišćenje memorije organizacije

Određeni elementi memorije organizacije moraju se proslediti relevantnim licima u kompaniji. Ova distribucija može biti pasivna ili aktivna. Bilo koji korisnik može samostalno pretraživati potrebne informacije na onim lokacijama gde su dostupne u kompaniji, ili će određeno lice ili grupa lica u kompaniji biti odgovorni za distribuciju znanja u kompaniji i sistematski odlučivati o tome. Kada radnici kompanije nemaju vremena da traže relevantne korporativne informacije, pasivna distribucija znanja je nedovoljna. Kuhn i Abecker preporučuju aktivnu distribuciju znanja. [244] Van Heijst, Van der Spek i Kruizing prema vrsti prikupljanja i difuzije memorije organizacije razlikuju nekoliko slučajeva: [229]

- „Potkrovlje znanja" – i prikupljanje i difuzija su pasivni.

- „Sunđer znanja" – prikupljanje je aktivna, ali difuzija je pasivna.
- „Izdavač znanja" – prikupljanje je pasivna, ali distribucija je aktivna, kako se elementi memorije organizacije prosleđuju relevantnim licima.
- „Pumpa znanja" – i prikupljanje i difuzija su aktivni (primer *ICARE* projekt) [301]

Pojedinci i kompanije mogu iskoristiti velike mogućnosti pristupa podacima, informacijama i znanju koje pruža Internet. Difuzija znanja može koristiti u eksploataciji mogućeg pristupa Internetu ili Intranetu unutar kompanije. Difuzija se može osloniti na znanja servera na *Web* ili na objavljivanju znjanja na *Web*. [231][286] Do različitih vrsta elemenata može se pristupiti kroz Internet ili Intranet: dokumente, baze podataka, ontologije, baze znanja, baze predmeta, članke digitalnih dnevnika itd. To nas upućuje da je moguće osmisliti nekoliko vrsta servera: serveri dokumenata, ontološki serveri, serveri baze znanja, serveri baze podataka, serveri dnevnika ili digitalne biblioteke. Glavni problemi su: pronalaženje elemenata memorije organizacije u odgovoru na zahtev i prilagođavanje odgovora korisniku. Za ovu svrhu može biti interesantno istraživanje o korisničkom profilu Sorensena i ostalih. [259]

Koristeći razliku između unutrašnje i spoljašnje memorije, moramo se podsetiti da memorija organizacije ne može biti ograničena na samu kompaniju. Unutrašnja memorija organizacije može se osloniti na internu mapu kompetencija unutar kompanije, dok spoljašnja memorija organizacije umesto toga uključuje informaciju i znanje koje proizlazi iz spoljašnjeg sveta, ali koje je korisno za poslovanje kompanije. Zbog toga, pronalaženje i integracija informacija eksplicitno postavljenih na Internet od strane drugih kompanija koje rade u istom području poslovanja može biti korisno za spoljašnju memoriju organizacije. Intranet u kompaniji može biti korišćen za konstrukciju i difuziju unutrašnje memorije organizacije, dok se spoljašnja memorija organizacije može osloniti na: Ekstranet koji povezuje kompaniju i neke povlašćene partnere. U svojim istraživanjima Revellianalizira različite vrste „inteligencije" koje su interesantne za kompaniju. [302]

Zbog potencijalnih problema kao što su poverljivost, bezbednost i pouzdanost pristupa informacijama treba imati u vidu da korišćenje resursa memorije organizacije preko Interneta i *Web*, predstavljaju rizik od viška informacija koje mogu ometati zaposlene u svom radu u kompaniji kao i kompromitovanja važnih informacija kompanije za njeno poslovanje.

6.7 Ocenjivanje memorije organizacije

Operativni projekti memorije organizacije su zahtevni i skupi [303]. Zato je vrednovanje i ocenjivanje takvih projekata važno, kroz nekoliko stanovišta: ekonomsko-finansijskog, socio-organizacionog i tehničkog. Sa ekonomsko-finansijskog stanovišta, jedan od ciljeva memorije organizacije je poboljšanje konkurentnosti kompanije. Kao što je navedeno u [246] poboljšanje konkurentnosti može se meriti dobitkom između uspeha proizvoda kompanije ili usluga, i troškova proizvodnje i održavanja. Potrebno je da postoji procena prihoda dobijenog zahvaljujući uvođenju memorije organizacije, generalno usmerene na povećanje produktivnosti kompanije. Sa stanovišta menadžera povraćaj ulaganja je važan za opravdanje korisnosti izgradnje memorije organizacije. Međutim, neophodne su metode ili alati za procenu stvarnog poboljšanja uvođenjem memorije organizacije. To može biti poboljšanje bezbednosti kroz izbegavanje grešaka iz prošlosti, ili poboljšanja u kvalitetu i performansama.

Sa socio-organizacionog stanovišta, memorija organizacije može imati za cilj poboljšanje organizacije rada zaposlenih i zadovoljstva zaposlenih. Međutim, kriterijumi za takvu procenu često su kvalitativni , a retko kvantitativni. Mogu se osloniti na klasične kriterijume koji se koriste za procenu alata usmerenih na korisnike, kao što je lakoća korišćenja informacija, lakoća pronalaženja informacija, adekvatnost preuzetih informacija, poverenje u takve informacije, upotrebljivost za aktivnosti korisnika itd. Kao što su u svojim istraživanjima primetili Kuhn and Abecker povratne informacije korisnika treba iskoristiti za otkrivanje mogućih nedostataka u memoriji organizacije i sugerisati ih za njeno poboljšanje. [244]

Sa tehničke tačke, prenos znanja i veština u okviru kompanije predstavlja se kao evidentna dobit. Ipak, efikasan prenos znanja zavisi od efikasne upotrebe memorije organizacije i njenog prilagođavanja prenosu znanja. U upotrebi memorije organizacije postoje određene predrasude jer uvođenje memorije organizacije može da podrazumeva promene u individualnom i kolektivnom radu u kompaniji. Isto tako, neke reorganizacije unutar kompanije koje propisuju menadžeri, zaposleni ne mogu da prihvate. Službeno postupanje za čuvanje znanja ili iskustava povezanih sa datim projektom mogu biti propisani od strane rukovodilaca kompanije, ali se ne poštuju iz razloga kao što su nedostatak vremena, nedostatak motivacije zaposlenih itd. Pored toga, memorija organizacije može se koristiti i na drugi način koji nije planiran. Retke su publikacije koje se bave analizom reakcije korisnika memorije organizacije.

Kuhn i Abecker u [244] analizirli su tri studije slučaja: KONUS za dizajn kolenastog vratila, RITA za osiguranje kvaliteta za komponente vozila i PS-savetnik za pripremu ponuda za naftni proizvodni sistem. Autori su primetili da sva tri sistema nisu uspela da prođu stadijum prototipa i nisu bili integrisani u svakodnevni operativni rad kompanije. Kao lekcija naučena iz studije ovih slučajeva, predloženi su ključni zahtevi za memoriju organizacije i opštu arhitekturu memorije organizacije i neka vrsta metodološkog vodiča za njen razvoj.

Kao zaključno razmatranje, prilikom ocenjivanja memorije organizacije moramo razlikovati procenu od strane korisnika i stratešku procenu od strane menadžera. Trenutno je malo efektivnih operativnih memorija organizacije, a kompanije moraju da se povuku sve dok se napravi precizna evaluacija – vrednovanje memorije organizacije.

6.8 Održavanje i razvoj memorije organizacije

Za održavanje i razvoj memorije organizacije, potrebno je uzeti u obzir rezultate vrednovanja rešenja koja već postoje. Problemi vezani za dodavanje novih znanja, uklanjanje ili modifikaciju zastarelih znanja, problemi koherencije koji podrazumevaju kooperativno proširenje memorije organizacije, samo su neki od problema koji se moraju rešiti u budućnosti i od kojih zavisi dalji razvoj memorije organizacije. Neki od navedenih problema već su bili razmatrani u poglavlju rada koji govori o izgradnji memorije organizacije. Pored toga, u razvoju memorije organizacije mogući su organizacioni i tehnički problemi. U izgradnji, kao i u razvijanju, mogu nastati određeni problemi zbog sukoba između ljudi, nedostatka komunikacije, nedostatka motivacije ili nedostatka vremena.

Tehnike koje se koriste za održavanje i razvoj memorije organizacije zavise i od same vrste memorije organizacije. U zavisnosti od posmatranog slučaja, dodavanja novih elemenata, uklanjanja ili modifikacije memorije organizacije, problemi u budućnosti će se odnositi na osnovne elemente znanja ili predmeta u bazi znanja ili (elemenata) dokumenata

u bazi dokumenta ili agenata u multi-agent sistemima memorije organizacije. Takođe, zavisi i od toga da li je difuzija elemenata memorije organizacije pasivna ili aktivna [229]. Na kraju moramo dodati još i da razvoj zavisi i od dizajnera i od korisnika memorije organizacije.

6.9 Problemi upravljanja sa velikom količinom podataka

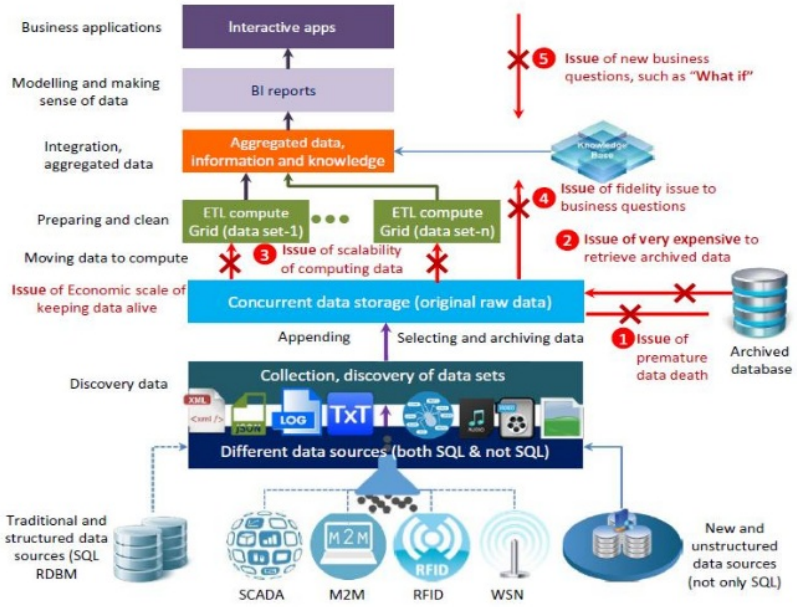
6.9.1 Big Data sistemi

Porast količine digitalnog sadržaja sa kojom se sreću savremene kompanije i pojedinci, nameće pitanje njihovog prikupljanja, klasifikacije, skladištenja i statističke obrade kao važan poslovni, a ne samo tehnički problem. Za kompanije su svi prikupljeni sadržaji potencijalno upotrebljivi i predstavljaju jedan od bazičnih resursa koji im omogućavaju pouzdano planiranje i upravljanje poslovanjem. [304] Da bi kompanije bile sposobne za nove načine poslovanja i funkcionisanja, neophodno je da vladaju novim tehnikama prikupljanja, obrade i postupcima dobijanja korisnih i pouzdanih zaključaka primenom statističkih metoda i alata [305]. Svi ovi podaci dobili su naziv *Big Data* i opisuju njihovo prikupljanje, obradu, analizu i skladištenje kroz korišćenje brojnih tehnika i tehnologija.

6.9.1.1 Pojava, definicija i karakteristike „Big Data" sistema

Kako bi ukazali na značaj vizuelizacije velikih skupova podataka koji su prevazilazili kapacitete za skladištenje, izraz *Big Data* prvi put su upotrebili 1997. godine Koks i Elsvort. [306] U literaturi se često može pronaći podatak, da su Vajs i Indurkia u cilju opisa rasta podataka i značaja savremenih tehnologija za rad sa velikim količinama podataka upotrebili izraz *Big Data* 1998. godine. [307] U formi u kojoj ga danas poznajemo *Big Data* je formulisao Rodžer Mugalas 2005. godine. [308]

U pokušaju da opišu i pojasne sam sistem postoje različite definicije *Big Data* različitih autora. Prva definicija *Big Data* sistema nastaje 2001. godine kada Laney ukazuje na izazove i mogućnosti koje donose dostupni podaci iz različitih izvora u velikim količinama i u realnom vremenu. [309] McKinsey institut definiše *Big Data* kao „bazu podataka čija veličina prevazilazi mogućnosti tradicionalnih baza podataka i softvera za prikupljanje, obradu, analiziranje i čuvanje podataka" [310]. Najčešće su ovi podaci nestrukturirani (datum, tekst, simboli) i polustrukturirani i čine 95% svih novih podataka. [311] Drugi autori su mišljenja da se ti podaci ne mogu smestiti u radnu memoriju računara [312] ili relacione baze podataka radi obrade [313].



Slika 35. *Ključne motivacije za „Big Data" analizu*
Izvor: [314]

U svojim istraživanjima Čen, Žang i Stori smatraju da su *Big Data* skupovi podataka koji su veliki i složeni te zahtevaju posebne i inovativne pristupe za njihovu manipulaciju. [315] Čen i Ženg su dali pregled vrhunskih tehnika i tehnologija koje se mogu prilagoditi rešavanju *Big Data* problema. [315] Ukazali su da ona može poslužiti kao katalizator za razvoj mnogih drugih oblasti, kao što su granularno računarstvo (engl. *Granular Computing*), računarstvo u oblaku (engl. *Cloud Computing*), bioračunarstvo (engl. *Bio-inspired Computing*), kvantni računari (engl. *Quantum Computing*), od kojih su neke već u upotrebi, dok su neke još uvek u fazi razvoja. [316] *Big Data* je u velikoj meri promenio način na koji se informacije obrađuju i primenjuju u procesu donošenja odluka. [317]

Možemo zaključiti da *Big Data* ne predstavlja jedinstvenu tehnologiju, već kombinovanu primenu novih i starih tehnologija tako da kompanije budu u mogućnosti da upravljaju velikim količinama različitih podataka adekvatnom brzinom i u odgovarajućem vremenskom okviru u svrhu analize podataka u realnom vremenu. *Big Data* karakterišu tri stvari (3V): količina/obim podataka (engl. *Volume*), brzina generisanja, prikupljanja, obrade i analize podataka (engl. *Velocity*) i raznovrsnost (engl. *Variety*).

Kada govorimo o količini/obimu podataka moramo konstatovati da postoji veliki broj faktora koji doprinose uvećanju obima podataka. Padom cene memorijskih uređaja skladištenje danas više ne predstavlja problem. Ipak, pojavili su se drugi problemi, kao što su određivanje važnosti određenih podataka u velikoj količini podataka. [318] Procenjuje se da ljudi na dnevnom nivou stvaraju 2,5 kvintiliona bajtova podataka [319].

Brzinu generisanja, prikupljanja, obrade i analize podataka karakterišu: brzina kreiranja podataka i brzina kojom podaci moraju biti obrađeni kako bi ispunili određene kriterijume. Na ovaj način se definišu novi pravci poslovanja kompanija po kojima se sve mora realizovati „sada i odmah" [320]. Prikupljanje, obrada i analiza podataka u realnom vremenu ima svoje prednosti koje se ogledaju u tome da: (1) kompanije mogu u svakom

trenutku dobiti informacije o greškama i propustima koji nastanu u kompaniji i preduzeti korektivne mere; (2) kompanije mogu odmah da saznaju koje nove strategije preduzimaju konkurenti i na osnovu toga izvršiti prilagođavanje svojih aktivnosti i poteza; (3) kompanije stiču uvid u reakcije kupaca, njihova mišljenja, stavove i komentare o proizvodima i uslugama i tako da mogu adekvatno odreagovati. [321]

Tabela 16. „*Big Data*" mogućnosti i njene primarne tehnologije
Izvor: [330]

***Big Data* mogućnosti**	**Primarne tehnologije**	**Karakteristike**
Skladištenje i sposobnost upravljanja	Hadoop Distributed File System (HDFS)	Distribuirani datetečni sistem iz otvorenih izvora. Pokreće se na hardverima sa visokim performansama. Visoko skalabilno skladištenje i automatsko replikovanje podataka
Mogućnosti baza podataka	Oracle NoSQL	Dinamičan i fleksibilan dizajn šeme, visoko skalabilan milti – čvor, višestruki podatkovni centar, tolerantnost grešaka, ACID operacije. Visoke ključ performase, Baza podataka o paru vrednosti
	Apache HBase	Automatska podrška za neuspeh između regionalnih servera. Automatsko i konfigurativno sređivanje tabela
	Apache Cassandra	Mogućnost tolerancije greške za svaki čvor. Indeksi kolona sa *log-structured updates* i *built-in caching*
	Apache Hive	Upit izvršenja preko MapReduce. Korišćenje SQL-like jezika HiveQL, Laki ETL procesi bilo od HDFS ili Apache HBase
Mogućnosti obrade	MapReduce	Distribucija opterećenja podataka preko hiljadu čvorova. Pretvara problem u manje pod probleme
	Apache Hadoop	Izuzetno prilagodljiva infrastruktura. Visoko skalabilna batch obrada. Pogrešna tolerancija
Mogućnost integracije podataka	Oracle Big Data konektori, Oracle Data Integrator	Izvoz MapReduce rezultira u RDBMS, Hadoop, i drugi ciljevi, uključujći Grafical User Interface
Mogućnosti statističke analize	R i Oracle R Enterprise	Programski jezik za statističku analizu

Karakteristika raznovrsnost odnosi se na raznovrsnost i posledičnu strukturu podataka [322]. Podaci su danas dostupni u različitim formatima [323] kao što su tradicionalne baze podataka, tekstualni fajlovi, e-mail, video, audio, podaci o finansijskim transakcijama, itd. Neke procene govore da oko 80% podataka nije numeričkog tipa, ali oni moraju ostati uključeni u procedure analize i donošenja odluka u vezi sa njima. [324] Svetski ekonomski forum istakao je značaj nestrukturiranih podataka za poslovanje kompanije i klasifikovao ih kao značajan resurs. [325]

U suštini, izraz *Big Data* ne odražava u potpunosti šta se tačno krije iza njega. Ključna osobina ovih podataka je promena njihove strukture što se ogleda u reči *big*. Veličina je subjektivna kategorija i razlikuje se od kompanije do kompanije.[328] Vodeći stručnjaci koji se bave *Big Data* tehnologijama, predložili su različite izrazekao što su *Intelligent Data* i *Nano Data*. Jedan od vodećih istraživača u oblasti *Big Data* Bernard Mar, predložio je primenu izraza *Smart Data*, tvrdeći da on kompletnije odražava sve atribute novih podataka. [329] Međutim, ni jedno od predloženih rešenja nije ušlo u masovnu upotrebu.

Veći broj definicija *Big Data* orijentisan je na tehnologije i alate potrebne za rad sa podacima koji imaju nove osobine. [331] One podrazumevaju generisanje vrednosti iz velikih količina podataka koje potiču iz različitih izvora i njihovo prikupljanje, analizu i

obradu. [332] U njima su zanemarene znanja i veštine neophodne za uspešnu primenu *Big Data* koncepta. Jedna od ređih definicija koja se bavi drugim aspektima *Big Data* predstavljena je u izveštaju Svetskog ekonomskog foruma prema kojoj *Big Data* predstavlja dugoročnu težnju kompanije da unapredi proces odlučivanja tako što će „donositi odluke zasnovane na podacima" [333]. Tehnologije i alati za rad sa *Big Data* predstavljaju neophodan, ali ne i dovoljan uslov, jer kompanije treba da imaju zaposlene sa neophodnim znanjima, veštinama i sposobnostima za rad sa *Big Data* kako bi u tome bile uspešne.

6.9.1.2 „Big Data" tehnike za rad

U savremenom načinu poslovanja kompanija rad sa podacima značajno je promenjen. Ovo se naročito odnosi na način generisanja, prikupljanja, obrade, analize, čuvanje i prikazivanje podataka. Promenom ključnih karakteristika podataka kojima kompanije prikupljaju podatke, njihova analitička obrada podataka postaje složena aktivnost. Analitička obrada podataka podrazumeva „primenu statističkih i kvantitativnih metoda, raznih eksplanatornih i prediktivnih modela i koncepata menadžmenta za analiziranje podataka".[334] Poslednjih nekoliko godina sve više se ističe značaj *Big Data* analitike.[4]

Danas su podaci prisutni u velikim količinama, odlikuju se nestruktuiranošću i dostupnošću u realnom vremenu. Suština analize proširena je sa uzorka na čitavu populaciju. Tu se nameće potreba novog i drugačijeg načina razmišljanja kako na osnovu raspoloživih podataka kreirati novu vrednost u kompaniji. [335] Rešenje za ove izazove pronađeno je u brojnim tehnikama za analitičku obradu podataka.

Najčešće primenjivane tehnike su iz oblasti mašinskog učenja, neuronskih mreža, metoda optimizacije, analize društvenih mreža, vizuelizacije i slično. [315] Formirana je lista *Big Data* tehnika za analizu podataka koju čine: A/B testiranje, pravila povezivanja, klasifikacija, klastering, genetski algoritmi, mašinsko učenje, neuronske mreže, analiza društvenih mreža, prediktivno modelovanje, regresija, obrada signala, prostorna analiza, simulacija, analiza vremenskih serija. [310]

Za opstanak i uspeh proizvoda i usluga na tržištu mišljenja i stavovi kupaca na društvenim mrežama postali su veoma važni. [337] Za potrebe analize ovih podataka u praksi se u velikoj meri koristi analiza raspoloženja (engl. *sentiment analysis*). Njome se analiziraju mišljenja, stavovi i emocije ljudi o određenom proizvodu, usluzi, kompaniji, događaju. [310] Sprovodi se primenom linearne i logističke regresija, neuronskih mreža, otkrivanjem značajno različitih podataka, analizom vremenskih serija i dr. [338] Kada posmatramo izvore podataka uočavaju se razlike u analiziranju struktuiranih podataka, tekstualnih podataka, podataka sa Web-a, multimedijalnih podataka, podataka na mreži, podataka sa mobilnih uređaja i dr. [339]

6.9.1.3 „Big Data" tehnologije za rad u praksi

Postoji veliki broj tehnologija koje su namenjene za praktičan rad sa *Big Data*. Prve alate za *Big Data* razvio je Google početkom 2000. godine. To je podstaklo pojavu drugih tehnologija i alata koji omogućavaju u realnom vremenu i na ekonomičan način prikupljanje, obradu, analizu i čuvanje velikih količina različitih vrsta podataka. [305]

Klasifikaciju tehnologija za rad sa *Big Data* razni autori predstavljaju na različite načine. Broj tehnologija za rad sa *Big Data* je u stalnom porasu jer se stalno pojavljuju nove tehnologije. Većina njih je međusobno zavisno i preklapa se. U tabeli 17 prikazan je pregled tehnologija za rad sa *Big Data* koji ih predstavlja pomoću nekoliko segmenata: *Big*

Data analizu, baze podataka, rudarenje podataka (engl. *data mining*), sisteme datoteka, programske jezike, pretragu, agregaciju i transfer podataka. [340]

Tehnologije za rad sa *Big Data* koje se najčešće upotrebljavaju su: *Hadoop*, *Map Reduce* i *Big Table*. Ove tehnologije obezbeđuju brzu i efektivnu obradu velikih količina podataka u realnom ili približno realnom vremenu. [341]

Tabela 17. *Pregled „Big Data" tehnologija*
Izvor: [340]

***Big Data* platforme i alati za analiziranje**	**Baze podataka/ skladišta podataka**	**Poslovna inteligencija**	***Data Mining***	**Fajl sistemi**
Hadoop MapReduce GridGain HPCC Storm	Cassandra Hbase (Hadoop alati) MongoDB Neo4j CouchDB Orient DB Terrastore FlockDB Hibari Riak Hypertable Big Data Hive (Hadoop alati) InfoBright Community Edition Infinispan Redis	Talend Jaspersoft Palo BI Suite/Jedox Pentaho SpagoBI KNIME BIRT/Actuate	RapidMiner/ Rapid Analytics Mahout (Hadoop alati) Orange Weka jHepWork KEEL SPMF Rattle	HDFS (Hadoop Distributed File System)
Programski jezici	***Big Data* pretraga**	**Agregacija i transfer podataka**	**Raznovrsni *Big Data* alati**	
Pig/Pig Latin R ECL	Lucene Solr	Sqoop (Hadoop alati) Flume (Hadoop alati) Chukwa	Terracotta Avro Oozie Zookeeper	

U *Big Data* eri veliki značaj za razumevanje i interpretaciju rezultata ima način na koji se oni prikazuju što je i jedan od razloga za uvođenje posebnih softvera za prikaz rezultata. Dobijene rezultate znatno je preglednije posmatrati i na osnovu njih donositi zaključke kreiranjem različitih vrsta tabela, grafikona i slika. Tehnika vizuelizacije prema Olshannikovu i ostalih su: [342]

- *Tag cloud*,
- *Clustergram*,
- *Motion charts*.

Prikazivanje željenih rezultata poslovanja prema zadatim kategorijama – lokaciji,

brendu, tržištu, menadžerima prodaje i slično vrši se primenom tzv. vrućih mapa (engl. *Heat Maps*). Pomoću kontrolnih panela se obezbeđuje prikaz grafikona od važnosti za proces donošenja odluka (engl. *Dashboard*). [342]

U cilju lakšeg otkrivanja zakonitosti u podacima i donošenja relevantnih zaključaka, većina alata i softvera za vizuelizaciju rezultata zasnovani su na ključnim principima kognitivne psihologije u smislu boja, veličine i prikazivanja odnosa između različitih varijabli. Lista najčešće primenjivanih softvera za vizuelizaciju predstavljena je na web-sajtu www.capterra.com. Najzastupljeniji softverski alati su: *Sisense*, *Glimpse*, *J Report*, *Tableau*, *Xtensio*, *Super Star Suite*, *Zegami*, *Activu*, *Advizor Analyst*, *An yChart*, *App Neta*, *Big Picture*, *BIRT i Hub*, *Bright Gauge*.

Prilikom obrade i analiziranja podataka danas je potrebno primenjivati drugačije pristupe. Postoji dosta *open-source* rešenja. Fokus kompanija uvek treba da bude na donošenju poslovnih odluka, a ne na raspoloživim i dostupnim tehnologijama. Iako *Big Data* tehnologije nisu neophodne ili u nekim slučajevima ne predstavljaju idealno rešenje za date poslovne potrebe, mnogi menadžeri prate moderne tendencije i nastoje da implementiraju i primene najnovije tehnologije u kompanijama. Treba imati u vidu da kompleksnost informacionih sistema kompanija raste sa pojavom i uvođenjem novih tehnologija. Prilikom donošenja odluke o implementaciji određene tehnologije u kompaniji na ovu činjenicu treba obratiti pažnju.

6.9.1.4 Faktori koji utiču na primenu „Big Data" tehnologija

Na primenu *Big Data* tehnologija utiču mnogobrojni faktori. Oni se mogu podeliti na eksterne i interne (tehnički i organizacioni). Interni faktori dele se na faktore koji su povezani sa upravljanjem podacima, razumevanjem podataka i kulture koja podstiče nastanak kompanije u skladu sa vođenjem podataka. [343] Važne karakteristike organizacione kulture kompanije vođene podacima su analitička obrada podataka kao ključna aktiva kompanije i liderstvo koje je zasnovano na činjenicama (dostupnim podacima).

Interni faktori se odnose na sposobnosti kompanije da na osnovu podataka kreira vrednost. Potrebna je izgradnja informacionog ekosistema u kompanijama koji će obezbediti implementaciju *Big Data* tehnologija i njihovu efikasnu primenu. [343] Iz razloga zato što dostupnost tehnologije i mogućnosti prikupljanja podataka nisu presudni faktori, veoma je bitno imati i organizacione pored tehničkih faktora (tabela 18). U poređenju sa tehničkim faktorima, organizacioni faktori suu većoj meri odgovorni za primenu i perspektivu *Big Data* tehnologija u bilo kojoj kompaniji. [1] Ta odgovornost odnosi se na definiciju strategije za primenu *Big Data* tehnologija, posvećenost menadžmenta i zaposlenih, obuku i razvoj zaposlenih, kao i prilagođavanje dimenzija organizacionog dizajna i parametara organizacione strukture.

Tabela 18. *Tehnički i organizacioni faktori koji utiču na primene „Big Data"*
Izvor: [1]

Tehnički faktori	Organizacioni faktori
Donošenje odluke implementacije *Big Data* tehnologije	Podrška i posvećenost rukovodstva
Prilagođavanje tehnološke infrastrukture	Prihvatanje *Big Data* tehnologija od strane zaposlenih
Sinhronizacija podataka iz svih izvora	Znanje i veština zaposlenih za rad sa *Big Data* tehnologijama
Integracija podataka u jedinstvenu bazu	Saradnja zaposlenih koji rade sa **Big Data** tehnologijama i drugih zaposlenih u kompaniji
Bezbednost podataka	Podsticanje zaposlenih da se orijentišu na podatke prilikom donošenja odluka

Eksterni faktori se odnose na doprinos vlade država i njenih institucija da kompanije mogu koristiti podatke slobodno i produktivno kroz pravni okvir za privatnost, korišćenje podataka, infrastrukturu, javnu percepciju i svest. [333] Možemo zaključiti da se *Big Data* vremenom ugrađuje u postojeće okvire ekonomije svake države s ciljem da ukupnu privrednu aktivnost podrži i usmeri ka daljem razvoju. [345]

6.9.1.5 Negativne implikacije upotrebe „Big Data" tehnologija

Velika količina podataka može se stvarati i koristiti u razne svrhe. Tu se postavlja pitanje privatnosti podataka jer su u jednom delu tog procesa uključeni i ljudi. Situacije u kojima se upotrebljavaju podaci često je kompleksnija i donosi istovremeno pozitivne i negativne posledice. Negativna implikacija primene *Big Data* tehnologija ogleda se u činjenici da mnogi autori poistovećuju *Big data* sa „informacionim zatvorom" [346] i „digitalnim zatvorom". [347] Kao rezultat nastaju profesionalne etičke smernice i propisi koji određuju kako se treba odnositi sa podacima. Iskustva su pokazala da nema lakih rešenja i da se odluke baziraju na kompromisu. Najčešći problemi vezani su za kontrolu, privatnost, bezbednost podataka, profilisanje i tehnološko upravljanje.

U pogledu privatnosti i bezbednosti podataka primena *Big Data* tehnologija otvara brojna pitanja i izazove. [348][349] Kompanije, ali i same države, svakog dana prikupljaju velike količine podataka o svojim građanima, klijentima i njihovim aktivnostima. Tako se stvaraju digitalni tragovi, nad kojima nemamo informaciju o tome kako se oni koriste. [350] Privatnost zavisi od konteksta u kome se upotrebljava i višedimenzionalan je pojam. Privatnost podataka podrazumeva zaštitu podataka tokom procesa njihovog prikupljanja i tokom njihove obrade i primene. U suštini odnosi se na „prihvatljive prakse s obzirom na pristup i objavljivanje ličnih i osetljivih podataka".[350] Ne postoji dilema da se koncept privatnosti u potpunosti menja. U tom pogledu, ovo pitanje dobija još više na značaju.

U savremenoj literaturi iz oblasti *Big Data* tehnologija zagovara se potreba da kompanije jasno definišu vlasništvo i pravila pristupa različitim podacima i izvrše implementaciju bezbednosne politike vezane za podatke.[351] Predlaže se novi vid zaštite ličnih podataka – „privatnost kroz odgovornost" umesto pristupa „privatnost uz odobrenje".[317] Prema stavovima Siegela rešavanje ključnih pitanja privatnosti podataka trebalo bi sprovesti kroz odgovore na sledeća pitanja[352]:

- čuvanje (engl. *retain*) – Koji podaci i koliko dugo se čuvaju?
- pristup (engl. *access*) – Ko ima prava pristupa i kojim podacima?
- deljenje (engl. *share*) – Koji podaci se mogu razmenjivati, sa kim i pod kakvim uslovima?

- spajanje (engl. *merge*) – Koje podatke međusobno možemo spajati?
- akcija/delovanje (engl. *react*) – Na koji način se može preduzeti neka akcija na osnovu podataka?

Kitchin u svojim istraživanjima tvrdi da je bezbednost podataka postala važan aspekt zaštite podataka, što se posebno odnosi na vrednost podataka (kako ličnih, tako i komercijalnih).[350]

Dugo vremena prisutna je praksa da se podaci koriste za profilisanje i upravljanje populacijama. Za potrebe bezbednosti i detekciju prevara, državne institucije izrađuju profile građana. Kompanije žele da razumeju kako njihovi postojeći i potencijalni klijenti razmišljaju i kako se ponašaju u cilju usmeravanja i proširivanja svog delovanje a sve cilju povećanja profita. [353] Kako bi smanjile finansijske troškove i povećale produktivnost, kompanije kupuju profile i kontakt podatke čime izbegavaju nepotrebno oglašavanje i usredsređuju se na ciljnu populaciju. [352]

Još jedan od nedostataka primene *Big Data* tehnologija je potpuno zanemarivanje iskustva i intuicije donosioca odluka i odlučivanje zasnovano na podacima. [9] Traži se odgovor na pitanje ko donesi odluku – ljudi ili algoritmi? [354] Bez obzira na raznolikost tehnika i metoda rada *Big Data* koje efikasne i neophodne, na ljudima je da donose poslovne odluke u kompaniji. [355][356] Uz puno poštovanje privatnosti građana, primena *Big Data* tehnologija treba da bude u skladu sa pojedinačnim, društvenim i kulturalnim. [357]

6.9.1.6 Značaj „Big Data" tehnologija

Za svaku kompaniju, ali i svaki sektor ekonomije, podaci i informacije su uvek bili značajni. [358][359][360][361] Napretkom tehnologije, došlo je do promene načina na koji se podaci prikupljaju, obrađuju, analiziraju i čuvaju, [362][363] a istovremeno kompanije postaju svesne mogućnosti za kreiranje vrednosti na osnovu podataka. [364][365][366] Na osnovu *Big Data* tehnologija moguće je interpretirati i podatke koji su u kvalitativnom obliku. [317]

Rastom dostupnosti i raznovrsnosti podataka, tehničkih mogućnosti za njihovu obradu i analizu, potencijal za generisanje strateške vrednosti zasnovan na podacima, danas je veliki. Podaci postaju resurs koji se smatra odgovornim za „revoluciju menadžmenta" [323], resurs ravnopravan „nafti i zlatu" [326], „poluga inovativnosti, konkurentnosti i produktivnosti" [310], „ključni pokretač inovacija i kreativne destrukcije" [367]. Navedeni stavovi su danas posebno aktuelni jer su savremene kompanije preplavljene velikom količinom podataka koja se sukcesivno povećava. [368]

Postoji nekoliko važnih karakteristika *Big Data* tehnologija koje mogu pomoći kompanijama da kroz njihovu primenu kreiraju vrednost na osnovu iskustava stečenih kroz praksu, a to su: [310]

- transparentnost – ogleda se u tome da su svi podaci u kompaniji i van nje dostupni na jednom mestu,
- eksperimentisanje u cilju identifikacije različitih potreba i želja kupaca,
- identifikacija različitih segmenata kupaca od strane kompanija, [1]
- podrška procesu odlučivanja pomoću automatizovanih algoritama kroz kontrolisane eksperimente za testiranje hipoteza i analizu razultata donetih odluka [304], što omogućava donošenje odluka koje su zasnovane na podacima,

[369][322]

- poboljšanje postojećih proizvoda i usluga, uvođenje novih, promena poslovnih modela, može dovesti do novog proizvoda kompanije, nove usluge koju pruža kompanija, poboljšanja karakteristike proizvoda kompanije, novog pristupa u formiranja cena i slično. [328]

Primenom *Big Data* tehnologija kompanije stvaraju mogućnost boljeg razumevanja svojih kupaca, zaposlenih, poslovnih procesa, partnera, ali i identifikacije svih aktivnosti u kojima su potrebna i moguća poboljšanja.[370][343] *Big Data* tehnologije omogućavaju kompanijama značajno smanjenje oportunitentnih troškova i izbegavanje rizika neuspeha na tržištu razmatranjem opcija i predloga za redizajniranje proizvoda u ranoj fazi njegovog razvoja. Pored toga, *Big Data* pruža stvaranje potpuno novih kompanija čiji je poslovni model zasnovan na podacima koje imaju velike mogućnosti rasta i razvoja u budućnosti. [304]

6.9.2 Sistemi za planiranje poslovnih resusrsa – ERP sistemi

Razvoj informaciono-komunikacionih tehnologija doveo je do pojave elektronskog poslovanja. To je izazvalo redefinisanje poslovnih procesa kompanija i njihovih informacionih potreba. Kao odgovor na ove nove izazove razvijeni su ERP sistemi (engl. *Enterprise Resource Planning, ERP*) u svrhu integrisanja i obrade informacija zasnovanih na praćenju poslovnih procesa u kompanijama. [371][372] Na taj način ERP sistem, u kompaniji i van nje, omogućava se optimalno korišćenje resursa koji su joj na raspolaganju, jer uspešnost poslovanja zavisi od njene prilagodljivosti promenama na tržištu.[373]

6.9.2.1 Definicije ERP sistema

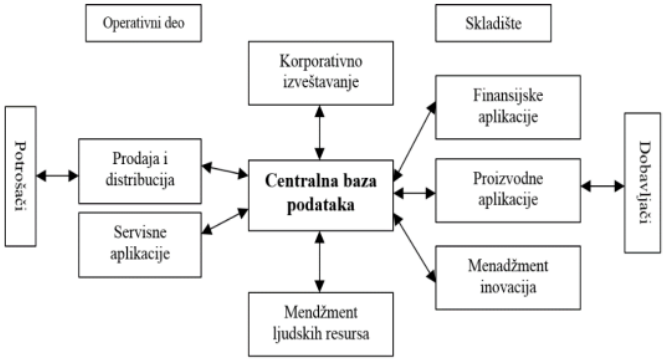
Pojam ERP se može tumačiti kao: [374]

- organizacija – kompanija (engl. e*nterprise*),
- resursi (engl. *resource*),
- planiranje (engl. *planning*).

Nije ga lako definisati, što navode Al-Mashari i ostali [375]. Boersma i Kingma [376] ukazuju da nema opšte prihvaćene definicije ERP sistema. Nakon navođenja desetak definicija od strane različitih autora, Klaus i ostali [377], takođe iskazuju dilemu mogućnosti i tačne definicije ERP sistema.

Pojam ERP uvela je 1990. godine Gartner grupa. Po njoj su ERP sistemi poslovne strategije i portfolio specifičnih poslovnih rešenja koji stvaraju vrednost za kupce i akcionare unapređujući međusobnu saradnju unutar i između kompanija na nivou operacionih i finansijskih procesa. [378] Kwahk i Ahn ERP sisteme vide kao visoko tehnički multifunkcionalne informacione sisteme koji su dizajnirani kako bi se povećala organizaciona radna uspešnost i konkurentnost produktivnim organizovanjem poslovnih procesa u cilju eliminacije dupliranog rada i podataka [379]. Monk i Wagner navode da je ERP strateški poslovni alat koji pomaže integraciji poslovanja kompanije pomoću računarskog okruženja sa centralizovanom bazom podataka prodaje i marketinga, proizvodnjom i upravljanjem materijalima, računovodstvom, finansijama i ljudskim resursima. [380] Po Leonu, ERP se može posmatrati kao predviđanje i balansiranje potražnje i nabavke kroz široku grupu poslovnih funkcija, koristi pravilno definisane postupke za donošenje odluka i koordinisanje različitih poslovnih akcija. [381] Zajednica američkih proizvođača i organizacija za brigu o robno-materijalnoj kontroli APICS (engl.

American Production and Inventory Control Society, APICS), definisala je ERP sistem kao okvir za organizovanje, definisanje i standardizaciju poslovnih procesa neophodnih za uspešan proces planiranja i kontrole organizacije, u cilju korišćenja internog znanje kompanija u težnji za sticanjem spoljašnjih 32ednosti. [382] Colmenares i Otineo pak smatraju da je ERP sistem integrisani skup programa koji pružaju podršku za osnovne organizacione aktivnosti, kao što su proizvodnja i logistika, finansije i knjigovodstvo, prodaja i marketing i ljudski resursi. [383] Hasibuan i ostali definisali su ERP sistem kao integrisani informacioni sistem namenjen podršci poslovnih procesa i upravljanje resursima unutar kompanije. [384] Prema Nah i ostali, može se definisati kao poslovni softverski sistem koji omogućava kompanijama uspešno i efikasno upravljanje upotrebe resursa pružanjem integrisanog rešenja za potrebe procesuiranja informacija kompanije. [385] Al-Fawaz i drugi, definišu ERP sistem kao rešenje koje omogućava kompaniji integrisanje svih osnovnih poslovnih procesa u svrhu poboljšanja efikasnosti i održavanja konkurentskog položaja. [386] Doom i Mils ga vide kao opsežni integrisani softverski sistem, koji podržava poslovanje kompanije. [387] Za 32venporta, predstavlja softver namenjen automatizaciji bazične aktivnosti kompanije, kao što su proizvodnja, ljudski resursi, finansije i upravljanje lancima nabavke, sjedinjavajući najbolju praksu čime omogućava brzo donošenje odluka, redukovanje troškova i veću kontrolu menadžera (slika 36). [388]



Slika 36. *Koncept ERP sistema*
Izvor: [389]

Kumar i Hillegersberg su definisali ERP kao konfigurisani informacioni sistem koji integriše informacije i na njima zasnovane proce32unutar funkcionalnih područja u kompaniji. [390] Beheshti smatra da je ERP skup poslovnih aplikacija ili modula, koji povezuju poslovne jedinice kompanije kao što su finansije, knjigovodstvo, proizvodnja i ljudski resursi u čvrsto integrisani sistem sa zajedničkom platformom i protokom informacija. [391] Tripathi definiše ER32istem kao sistem koji vrši integraciju primarnih poslovnih aplikacija, pri čemu one dele zajednički set podataka koji je sačuvan u centralnoj bazi podataka. [392] Prema Sheu i ostalima, integriše centralnu bazu podataka i svih modula [393].

Ross [39432 ostali idu korak dalje i ERP vide kao sistem upravljanja koji obuhvata integrisani skup softvera, koji se može koristiti za upravljanje i integrisanje svih poslovnih funkcija unutar kompanije sa specifičnom racionalizovanom arhitekturom podatkov32 integracije poslovnih procesa i razmenjivanju podataka sa kupcima. [395] Dhiraj tvrdi da je ERP sistem prvenstveno industrijski pojam za širok skup aktivnosti potpomognutih višestrukim modulima aplikacionog softvera koji pomaže proizvodnim, ali i drugim

menadžerima. [396]

U sklopu sveobuhvatne definicije ERP, interesantno je navesti definiciju ERP II sistema koju su dali Bond i ostali [397]. Oni ERP II definišu kao poslovnu strategiju i skup narednu generaciju aplikacija koje jačaju vrednost kupaca i deoničara osposobljavajući i optimizujući kompaniju kroz saradničku aktivnost i finansijske procese.

Na osnovu navednih definicija može se zaključiti da ERP sistem opisuje povezanost između velikog broja funkcija i procesa na jedinstvenoj osnovi za podatke pri čemu se obrada podataka odvija u realnom vremenu. Pomenuti procesi i funkcije odvijaju se kroz module, što takođe definiše ERP kao sistem. Dodatno, ERP sistemi poseduju sposobnost praćenja organizacionih promena kompanije u kojima je nezaobilazno uključen proces simulacije.

6.9.2.2 Evolucija ERP sistema

Dugogodišnji rad na optimizaciji upravljanja poslovnim procesima, optimalnom korišćenju raspoloživih resursa i razvoju informacionih tehnologija rezultirao je pojavom savremenih ERP sistema. [397] Pre pojave MPR sistema, osnovna tehnika za upravljanje zalihama, bila je EOQ (engl. *Economic Order Quantity, EOQ*). Prvi pokušaji za upravljanje resursa i potreba poslovnih sistema je razvijanje MRP sistema (engl. *Material Requirements Planning, MRP*) šezdesetih godina 20. veka. [398] To su bili računarski sistemi sa zadatkom unapređivanja poslovnih kontrola zaliha i sistema za planiranje proizvodnje. [399]

Potreba za integracijom poslovnih komponenti u jedinstveni sistem za planiranje, izvršenje i kontrolu proizvodnje, sedamdesetih godina 20. veka izazvala je primenu modifikovane MRP metode sa povratnom vezom (engl. *Closed Loop MPR*). [400] U drugoj fazi osamdesetih godina 20. veka razvijen je MPR II (engl. *Manufacturing Resource Planing, MPR II*) sistem koji je u sebi nosio i problem planiranja procesa proizvodnje. [389][401][402] Početkom devedesetih godina 20. veka novi ERP sistemi su praktično predstavljali integraciju koordinacije i integracije međuprocesa u korporacijama. [403]

Možemo primetiti da je u toku nova evolucija sistema za planiranje proizvodnje čija je glavna karakteristika reakcija dobavljača ERP sistema na stroge kriterijume konkurentnosti velikih poslovnih sistema. Ona se uočava u najmanje tri segmenta: širenju poslovnih procesa van granica korporacije, vertikalnoj specijalizaciji industrijskih ERP rešenja i razvoju komponentne arhitekture. [404] Savremeni ERP sistemi sadrže komponente sistema interakcije sa potrošačima CRM (engl. *Customer Relationship Management, CRM*) i komponente upravljanja lancem snabdevanja SCM (engl. *Supply Chain Management, CRM*). Dobavljači vrše aktivno prilagođavanje svojih rešenja za primenu u različitim industrijskim sektorima, putem prilagođavanja postojećih funkcija i dodatkom novih koje su specifične za određenu industriju. Ovi trendovi doprinose smanjenju standardnih troškova implementacije i približavaju ERP sisteme manjim i srednjim kompanijama. Vrši se transformacija u modularne arhitekture otvorenog tipa, čime integracija postojećih (engl. *legacy*) sistema postaje lakša i brža, a dodavanje novih modula i održavanje verzija aktuelnih normalna aktivnost. [405]

6.9.2.3 Arhitektura ERP sistema

Većina ERP sistema je zasnovana na klijent-server (engl. *Client/Server*) arhitekturi, pri čemu elemente ERP integracije sačinjavaju: baza podataka, softverski sistemi, korisnički interfejs, alati i poslovni procesi. Uspešnost procesa implementacije sistema,

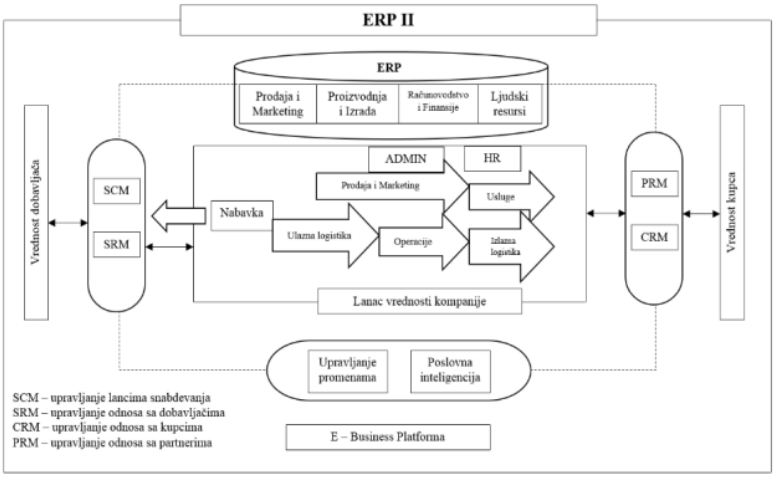
koja zahteva odgovarajući strateški, taktički i operativni pristup planiranju svih segmenata ekosistema informacija direktno je uređena specifičnošću strukture. [406] Slojevitost arhitekture omogućava istovremeni pristup podacima mnogih korisnika, čime se umanjuje rizik od pada sistema. Razlikuju se dvoslojne, troslojne i Internet arhitekture ERP sistema. Dvoslojnu arhitekturu čine: prvi sloj (odnosi se na server) i drugi sloj (odnosi se na klijenta). [373]

Kako može biti više korisnika, tako i klijenti koji su međusobno povezani mogu biti distribuirani na više mesta, pa su i ERP aplikacije postavljene na distributivni ili disperzivni način.

Klijent-server arhitektura većine ERP sistema sastoji se iz: [373]

- sloja prezentacije (engl. *Front Tier*) – koji predstavlja grafički korisnički interfejs ili veb pregledač za unos podataka ili pristup sistemu;
- sloja aplikacije (engl. *Middle Tier*) – pravila, funkcija, logike i ponašanja programa prilikom razmene podataka od/do servera baze podataka;
- sloja baze podataka (engl. *Back Tier*) – upravljanje operacijama i transakcijama podataka primenom DBMS i SQL.

Podaci koji se procesuiraju i skladište u sistemu, kritični su i osetljivi, i za to je odgovorna bezbednost sistema. Ona se može prikazati u obliku piramide. Osnovu predstavlja fizička bezbednost hardvera, baze podataka i medija za skladištenje podataka. Drugi nivo radi sa operativnim sistemom. Treći nivo orijentisan je na bezbednost softvera koja se postiže instalacijom bezbednosnog proizvoda ili njegovom ugradnjom u operativni sistem. Svrha ovog nivoa je da obezbedi prostor na disku i uputi informaciju operativnom sistemu i hardveru kako da spreči direktni pristup operativnom sistemu i hardveru preko ERP sistema. Ovaj nivo doprinosi i bezbednosti informacionog okruženja. Ako je ono bezbedno, ERP sistemi će poboljšati finansijski i operativni integritet osetljivih transakcija, u suprotnom, njihov integritet će biti narušen. Četvrti nivo predstavlja relacionu bazu podataka do koje se pristupa struktuiranim jezikom upita SQL (engl. *Structured Query Language, SQL*). Vrh piramide je ERP sistem (slika 37). [407] [408]



Slika 37. *ERP II idejni model*
Izvor: [408]

ERP sistem podrazumeva mnoge sigurnosne mehanizme kao što su zaštita pristupa podacima, provera korisničkih ograniče, autorizacija korisnika za određene transakcije. U odnosu na standardnu centralnu bazu podataka i ERP sistem razlika je u tome što se kod centralne baze podataka, informacije prikupljaju iz različitih funkcionalnih oblasti, odakle se one dalje „dele", dok su kod ERP sistema funkcionalna područja povezana sa centralnom bazom, ali i međusobno čime se otvaraju mogućnosti deljenja informacija kao kod centralizovane baze podataka, ali i procesno, između funkcionalnih jedinica, što je jedinstvena odlika ERP sistema. Ovakvim pristupom obezbeđuje se prava optimizacija resursa i ostvarenje poslovnih benefita.

6.9.2.4 Karakteristike ERP sistema

Zahtev za povećanje efikasnosti proizvodnje bila je osnovna motivacija evolucije ERP sistema tako da danas ERP sistemi obuhvataju sve poslovne funkcije. Cilj je integracija svih delova i funkcija kompanije u jedan sistem, koji može ispuniti specifične potrebe različitih vrsta korisnika. Zajedničkom operativnom bazom podataka za sve aplikacije i skladišta podataka koja obuhvata sve poslovne funkcije u kompaniji, obezbeđuju se potpuni i integrisani podaci i daje snažna podrška procesu odlučivanja u kompaniji. [373]

Imajući u vi osnovnu karakteristiku ERP sistema koja se ogleda u integrisanom planiranju i kontroli svih relevantnih resursa jednog poslovnog sistema, javlja se zahtev da svaki poslovni informacioni sistem treba da ima sledeće karakteristike:

- fleksibilnost i prilagodljivost,
- nazavisnost i sveobuhvatnost,
- modularnost i otvorena arhitektura,
- dostupnost i
- mogućnost simulacije realnih poslovnih okolnosti. [373]

6.9.2.5 Implementacije ERP sistema

Razmatrajući implementaciju ERP sistema Bredford je utvrdio da je to veoma složen i dugotrajan proces koji je vezan za mnoge riz e. [409] Na proces implementacije ERP sistema potrebno je obratiti veliku pažnju jer za razliku od ostalih informacionih sistema, implementacija podrazumeva transformaciju poslovnog sistema kompanije u manjoj ili većoj meri. Kumar i ostali z ljučuju da kompanije u svrhu održavanja konkurentske prednosti vrše neprekidnu analizu svojih poslovnih procesa i njihovo unapređenje (engl. *Business Process Improvement, BPI*) a po potrebi i reinženjering poslovnih procesa, nezavisno od informacionih sistema i ERP rešenja. Analizirajući procese čija je potrebna transformacija, kompanije posebnu pažnju poklanjaju procesima *Tri C* (engl. *Three Cs – customer, core, competition*). [410]

Prilikom rasrava o osnovama ERP sistema nezaobilazna činjenica je integracija i sistematizacija poslovnih funkcija, procesi podataka u jedinstveno okruženje kompanije. Za poslovne procese koji su nasleđeni nemoguće je izvršiti implementaciju gotovog ERP sistema bez nekog prilagođavanja. Uvođenje je po pravilu skup projekat. Sam ERP sistem treba da se realizuje integracijom i sistematizacijom poslovnih procesa i podataka, a koji za cilj ima značajne koristi za kompaniju. Khvalev tvrdi da opravdanost implementacije daje osnovne pretpostavke i sveobuhvatnu analizu troškova i koristi (engl. *cost/benefit*). Pored, što preciznije definisanih ciljeva i troškova koji prate realizaciju, javlja se potreba utvrđivanja i predviđanja svih rizika. Ako su u odnosu na pozitivne efekte implementacije

ograničenja i rizici preveliki, jedina ispravna odluka je napuštanje projekta. [411]

Upravljanje promenama predstavlja najveći trošak i ključni faktor rizika u implementaciji ERP sistema tvrdi Haddara. [412] Kroz unapređenje ili reinženjering poslovnih procesa, transformacija poslovnog sistema dovodi do radikalnih promena u načinu funkcionisanja poslovnog sistema kompanije što najviše pogađa neposredne izvršioce. Transformacija poslovnih procesa osim neposrednih izvršilaca, tiče se i svih ostalih *stejkholdera*. To implicira težnju za ostvarivanje što većih efekata na poboljšanje performansi poslovnog sistema uz što manje funkcionalnih promena. [413]

U implementaciji ERP sistema identifikovani su sledeći organizacioni problemi: neefikasno upravljanje strateško planiranje, otpor na promene, pogrešan izbor aplikacije, konflikti u kompaniji, nedovoljna podrška menadžmenta, troškovi implementacije i uticaj faktora kulture i okruženja. U svojim istraživanjima Yusuf identifikuje operativne, tehnološke i kadrovske probleme. [414]

Za implementaciju ERP sistema postoje različite strategije, koje se razmatraju već u ranoj fazi planiranja i izbora softverskog sistema i u njega moraju biti uključeni svi partneri u procesu implementacije i potencijalni dobavljači. [415] Vreme procesa uvođenja je različito i uslovljeno velikim brojem činilaca, a najčešće zavisi od izabrane strategije implementacije. Jedan od mogućih pristupa, koji zagovaraju Parr i Shanks je primena tri različite strategije implementacije: *Big Bang*, fazne ili modularne i *Slam dunk*. [416]

Big Bang strategija predstavlja ambiciozan i težak pristup implementaciji ERP sistema. [417] U nje se vrši jednovremena implementacija svih modula i podrazumeva jedinstven datum puštanja sistema u rad. Orijentiše kompaniju na kraći period uvođenja sistema i traži znatno više resursa za realizaciju projekta. Ova strategija je dala veoma mali procenat uspeha. Dobre strane su: kratko vreme implementacije i brži povrat investicije, a nedostaci se ogledaju u detaljnom planiranju, brzom prilagođavanju promenama, manjem vremenu za osposobljavanje zaposlenih, a greške na jednom delu sistema mogu se odraziti i na druge njegove delove.

Fazna ili modularna implementacija (engl. *Phased Rollout or Modular Implementation*) predstavlja najčešći i često najdugotrajniji pristup implementaciji. U osnovi primenjuju se kroz tri fazne primene: po modulima, prema poslovnim jedinicama i prema lokacijama. [417] Prednosti ove implementacije ogledaju se u tome da korisnici imaju više vremena za prihvatanje novog sistema, dok se tehnička lica unutar projektnog tima mogu usredsrediti na deo sistema ili grupu korisnika, a iskustvo na prvoj fazi primene koristi se u sledećim fazama tako da ostaje dovoljno vremena za učenje novih modula. Nedostatak ove implementacije ogleda se u nedovoljnoj fokusiranosti na primenu, duže vreme projekta, problematično održavanje postojećeg sistema i povezivanje sistema i novog rešenja.

Pod *Slam dunk* strategijom se podrazumeva implementacija ERP sistema u domenu jednog broja ključnih procesa, biranjem i prilagođavanjem, ukoliko je to potrebno, postojećim poslovnim procesima. [417] Ima nizak rizik neuspeha jer se ne vrši značajan reinženjering poslovnih procesa, već se samo uvodi nov alat za njihovu podršku. Fokusirana je na nekoliko ključnih procesa i podrazumeva da ERP diktira njihov dizajn.

Hibridna strategija je određena faznom implementacijom u horizontalnom i vertikalnom smislu. U kombinovanom pogledu se primenjuje u velikim korporacijama koje karakterišu mreža udaljenih poslovnih jedinicia sa relativno velikim stepenom autonomije upravljanja. [417][418]

Kompanije koje se upuštaju u projekat implementacije treba da budu spremne na

dugotrajni proces koji može potrajati više godina nezavisno od proizvođača ERP softvera, koji iz konkurentskih razloga, često ističu da je neophodno vreme za implementaciju sistema od tri do šest meseci,.

6.9.2.6 Standardi tehnologije realizacije ERP sistema

Brz tehnološki razvoj u oblasti informacionih tehnologija, donosi brže pojavljivanje novih tehnoloških standarda i smenjuje inicijative za standardizaciju tipičnih grupa problema i slojeva arhitekture jednog savremenog ERP sistema. Brojne formalne i neformalne inicijative dovele su do pojavljivanja grupe standarda rešenja za realizaciju različitih slojeva ERP sistem.

U sloju prezentacije podataka, najvažniji standardi su: XML (engl. *eXtensible Markup Language, XML*) i BPEL (engl. *Business Process Execution Language, BPEL*), koji predstavljaju osnovno sredstvo za prikazivanje i razmenu podataka o različitim procesima na struktuiran način, putem web servisa.

U aplikativnom sloju ERP sistema vrši se primena programskih jezika četvrte generacije. Najrasprostranjenija programska platforma za razvoj ERP sistema je J2EE (*Java 2 Platform Enterprise Edition, J2EE*). Njen prodor na tržištu ju je učinio dominantnom u odnosu na ISO (*International Standards Organization, ISO*) ili ECMA (*European Computer Manufacturers Association, ECMA*) propise i danas je čak osnova za sertifikaciju ERP sistema (engl. *J2EE compliance*).

Sloj skladištenja podataka, odnosno integrisanja aplikativne logike sa serverima baza podataka uključuje dominantne standarde: JDBC (engl. *Java Database Connectivity, JDBC*), ODBC (engl. *Open Database Connectivity, ODBC*), ADO (engl. *Active Data Objects, ADO*), OLE/DB (engl. *Object Linking and Embedding / Database, OLE/DB*) i ODBO (engl. *Object Linking and Embedding Database for Online Analytical Processing abbreviated, ODBO*).

Formulisanje i razvoj standarda u domenu interoperabilnosti komponenata poslovnog informacionog sistema trenutno je oblast u kojoj se najviše istražuje. Sloj integracije ERP sistema karakteriše rastuća primena odgovarajućih standardnih metoda i procedura *Web* servisa. Najznačajniji standardi uovoj oblasti su SOAP (engl. *Simple Object Access Protocol, SOAP*), UDDI (engl. *Universal Description Discovery and Integration, UDDI*) i WSDL (engl. *Web Services Description Language, WSDL*).

6.9.2.7 Rešenja ERP sistema

Danas postoje više komercijalnih ERP rešenja, a na stotine *open source* rešenja. Obzirm da na globalnom tržištu postoji velik broj poizvođača ERP softvera, ovde ćemo navesti one koji su u većoj meri prisutni na tržištu Srbije. Među vodećim svetskim proizvođačima ERP sistema vlada velika konkurencija, tako da SAP rešenje predstavlja tržišnog lidera a slede ga *Oracle*, *SAGE*, *Infor* i *Microsoft* kao i niz manjih proizvođača. Svaki od ovih proizvođača ERP sistema ekspert je za određeni modul. [419]

Tabela 19. *Zajednički ciljevi proizvođača i korisnika ERP sistema*
Izvor: [420]

Cilj	ERP proizvođač	ERP korisnik
Kvalitet (funkcionalnosti) rada	Želi da zadovolji najviše poslovne standarde kroz implementaciju specijalizovanog ERP sistema (shodno potrebama klijenta) i definiše novo poslovno okruženje kroz razvoj novih funkcionalnosti	Zahteva realizaciju svojih zahteva na što bolji, brži i kvalitetniji način, kroz standardizaciju poslovanja i definisanja novih funkcionalnosti
Brzina	U što kraćem vremenskom intervalu uspešno implementirati ERP sistem kod korisnika (radi oslobađanja resursa za nove projekte i dobrog ličnog marketinga, reference)	Želi da imlementira ERP sistem ranije i brže od svojih konkurenata, i time stekne konkurentnu prednost na tržištu
Uspeh klijenata u ostvarivanja poslovnih ciljeva	U želji da razvije svoje poslovanje potrebno je da ERP proizvođač ima zadovoljne i usešne klijente	Vidljive poslovne dobiti koje nastaju kao direktni rezultat rada implementiranog sistema

Domaći proizvodi na ERP tržištu su: *M&I Systems* – MIS ERP, *IIB-UPIS.net*, *Saga-Avizo*, *ASW-asw:dominus*, *Breza-Breza ERP*, *ABsoft*-ERP, *OSA-UBB*. U velikoj meri su slični i razumevanje svakoga od njih zahteva dugogodišnji konstantni rad. Potrebno je fokusirati se na karakteristike integrisanih informacionih sistema.

Cloud platforme predstavljaju tendenciju u oblasti ERP sistema. Menadžeri organizacije u svrhu redukcije troškova i smanjenja pojave grešaka u kanalu lanca trebali bi da izdvoje dovoljno resursa za virtuelno poslovanje i razmotre upotrebu ovog alata.

6.9.2.8 Prednosti i nedostaci ERP sistema

Po Yajunu, u post implementacionom periodu postoji pad performansi ERP sistema [421]. Rezultati njegove studije su potvrdi da se neposredno nakon implementacije kod jednog broja firmi javlja pad performansi sistema, koji traje od nekoliko nedelja do skoro godinu dana. Za unapređenje poslovanja implementaciju ERP sistema treba uspešno realizvati. Prednosti ERP sistema čini: [422]

- lak pristup informacijama koje su pouzdane;
- eliminacija bespotrebnih podataka i operacija;
- smanjenje vremenskog ciklusa;
- povećana efikasnost;
- smanjenje troškova i
- lak proces prilagođavanja promenama poslovnog okruženja.

Istovremeno, nedostaci ERP su:

- skupa i dugotrajna implementacija;
- nametnuta adaptacija organizacije i
- zavisnost od jednog dobavljača ERP rešenja.

I pored svojih nedostataka, implementacija ERP rešenja predstavlja dobru investiciju za kompaniju, jer se smanjenjem troškova i boljom organizacijom vraća novac uložen u kompaniju. Ukupne performanse kompanije se poboljšavaju objedinjavam poslovnih procesa uz visok stepen integracije modula zaduženih za praćenje poslovanja. [423] ERP omogućava usklađivanje strategijskih projekcija i taktičkih planova i zadataka,

ali i stvaranje veza između ljudi, procesa i tehnologije sa organizacionim ciljevima. [424]

6.9.3 Data Warehouse sistemi

Pitanja dobijanja informacija na osnovu kojih se donose poslovne odluke, često zahtevaju ukrštanje podataka koji su u kompanijama disparitetni. Ovaj i mnogi drugi problemi, doveli su dorazvoja velikih skladišta podataka (engl. *Data Warehouse*) čiji je cilj da u jednom poslovnom okruženju prvo izvrše integraciju različitih izvora podataka, a zatim omoguće brzo i lako izvršavanje različitih analitičkih operacija nad takopovezanim podacima u cilju donošenja pravovremenih poslovnih odluka u kompaniji.

6.9.3.1 Osnovni okviri skladišta podataka

Pod skladištima podataka (engl. *Data Warehouse*) podrazumeva se zbirka podataka izolovanih iz operativnih baza i sačuvanih u posebne baze – skladišta podataka. Ralph Kimball navodi definiciju skladišta podataka kao kopije transakcionih podataka specifično struktuiranih za upite i analize. [425] Glavna odlika koja određuje skladište podataka odnosi se na njegovu svrhu. Skladišta podaka prikupljaju i organizuju podatke tako da oni budu lako dostupni u cilju brze i jednostavne upotrebe za analizu poslovanja. [425][426]

Za Inmona „*data warehouse* je kolekcija podataka, koja omogućava donošenje poslovnih odluka, a koja je: subjektno orijentisana, integrisana, sadržajno nepromjenljiva i osetljiva na protok vremena". [427] Stiče se utisak da su osobine koje *data warehouse* treba da ima u funkciji formiranja informacionog sistema koji sa izvorinim sistemima od kojih dobija podatke ima *low coupling* komunikaciju. [428]

Proces smeštanja podataka u skladišta podataka je kontinuirani proces planiranja i prikupljanja podataka iz različitih izvora, kao i njihovog korišćenja, održavanja, upravljanja i konstantnog unapređivanja. Njega karakteriše vizija o tome šta se želi postići kreiranjem skladišta podataka. Jedna od ciljeva skladištenja može biti razvijanje i korišćenje znanja zasnovanog na podacima (engl. *data-based knowledge*). [429]

Investicija uvođenja skladišta podataka je skupa i dugotrajna. Prilikom procesa donošenja odluke o implementaciji skladišta podataka važno je izvršiti usaglašavanje o nizu bitnih pitanja za uspostavljanje projekta skladišta. Pre implementacije potrebno je uočiti poslovni interes za izgradnju i upotrebu skladišta podataka u skladu sa potrebama svog poslovanja. Nakon toga potrebno je dogovoriti izvore finansiranja procesa uvođenja i razviti kriterijume za održivanje poslovne upotrebljivosti skladišta podataka. Važno je doneti odluku o veličini skladišta podataka, utvrditi sa aspekta sadržaja vrstu skladišta, odrediti fizičku lokaciju i doneti odluku o izgradnji ili kupovini skladišta podataka. Potrebno je napraviti izbor najpovoljnijih alata i sistema za upravljanje bazama podataka, kao i rešiti pitanje zapošljavanja itd. Nakon implementacije sistem započinje sa radom i sprovodi se obuka korisnika u cilju pravilnog korišćenja instaliranih alata i upravljanja sistemom skladištenja.

6.9.3.2 Cilj realizacije skladišta podataka

Ukrštanje informacija koje se nalaze u operativnim bazama podataka sa informacijama iz ostalih eksternih izvora podataka predstavlja glavni cilj skladišta podataka. Kao vodeći autoritet u oblasti skladišta podataka Kimbell se osvrnuo na nekoliko ciljeva implementacije skladišta podataka: [425]

- Mora da obezbedi da podaci budu lako dostupni krajnjem korisniku.
- Podaci moraju biti konzistentni.

- Osvežavanje skladišta podataka, odnosno, ažuriranje novim podacima treba biti kontinuirani proces.
- Skladište podataka mora da bude adaptivno na promene koje zahtevaju korisnici.
- Podaci moraju da budu zaštićeni u skladištu.
- Skladište podataka mora da unapredi donošenje odluka u kompaniji.
- Korisnici moraju da prihvate rad sa skladištima podataka.

6.9.3.3 Osnovne funkcije skladišta podataka

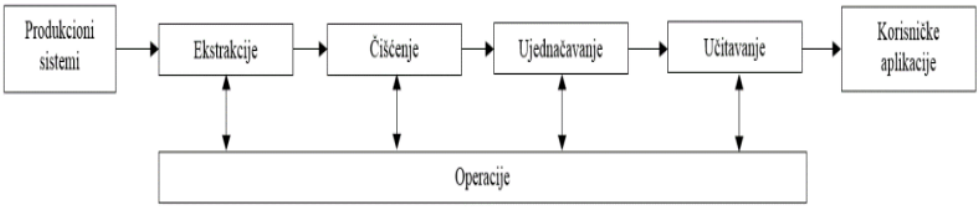
Primenom skladišta podataka vrši se rasterećivanje operativnih baza podataka složenih upita, tako da dolazi do unapređenja njihovih funkcija. Iz operativnih baza najčešće se vrši uklanjanje velike količine istorijskih podataka koji migriraju u skladišta podataka. Informacioni sistem kompan[41] u tom slučaju čine dva dela: operativni deo i skladište podataka. Koristeći tehnike otkrivanja znanja skladište podataka pruža stalno pronalaženje novih informacija u zavisnosti od novonastalih uslova i zahteva. Procesi za kreiranje informacija (ekstrakcija, agregacija, analiza, izveštaji itd.) se izdvajaju iz operativnih procesa, što ukazuje da operativni nivo sistema više nije opterećen njima. Tada skladište podataka postaje mesto sakupljanja i skladištenja poslovnih podataka i izvor informacija korišćenih prilikom poslovnog odlučivanja. [430]

Skladišta podataka se sastoje iz dva osnovna dela, a to su podaci i mehanizmi manipulacije tim podacima. U delu gde se nalaze podaci javljaju s[41]osnovni podaci i agregirani višedimenzionalni podaci, dok mehanizme obrade čine procesi ekstrakcije, transformacije i punjenja podataka, (ETL) sistem upravljanja podacima, postupci analitičke obrade podataka i sama prezentacija podataka.

Osnovna namena im je sakupljanje podataka i stvaranje logički integrisanih i predmetno usmerenih informacija. Skladište podataka treba oblikovati na način da se jednostavno i brzo može prilagoditi svim promenama i zahtevima poslovnog okruženja kompanije. Pre[7]a delovanju skladišta, a s obzirom na predmetnu usmerenost podataka, primenjuju se tehnike koje podržavaju predmetnu orijentaciju i obezbeđuju dovoljnu prilagodljivost kako bi se tokom vremena u skladište mogli integrisati i poda[8] iz mogućnih dodatnih izvora. U današnjem načinu poslovanja skladište podataka je izvor stabilnih podataka, nezavisnih od eventualnih promena u poslovnim procesima. To je razlog zašto je potrebno koristiti model otporan na uticaje operativnih procesa koji stvaraju [8]ćinu podataka. Izolovanjem skladišta podataka od operativnih obrada, obezbeđuje se unapređenje procesa generisanja informacija. Kroz tehnike otkrivanja znanja skladište podataka obezbeđuje stalno pronalaženje novih informacija. [430]

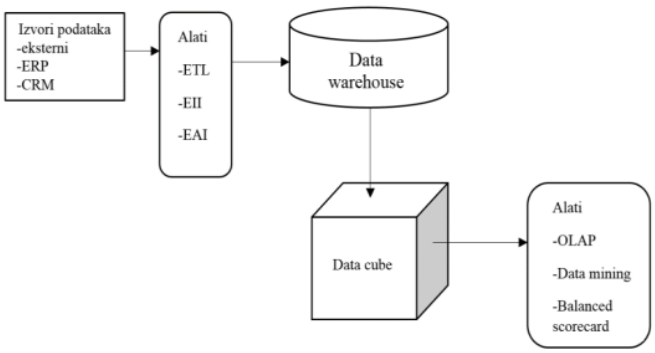
6.9.3.4 ETL procesi

Ulaz podataka u skladište vrši se iz različitih izvora, a najčešće iz transakcionih sistema kompanije. Procesi integrisanja podataka i organizovanje njihovih sadržaja pred[41]lja najopsežniji posao u aktivnostima skladištenja podataka. Glavnu ulogu u tome čini skup procesa čiji je zadatak da zahvate, preoblikuju i izvrše punjenje, odnosno unos podataka iz jednog ili više produkcionih sistema u skladište podataka. [178] Ovakav sled stvari se naziva ETL proces, skraćeno od ekstrakcija, transformacija i punjenje (engl. *extract, tr[9]sform, load, ETL*) [431]. Prilikom izgradnje ETL sistema treba se fokusirati na dva toka, koja se paralelno odvijaju a to su: tok planiranja i projektovanja ETL procesa i tok podataka u ETL procesu (slike 38 i 39).



Slika 38. *Tok podataka u ETL procesu*
Izvor: [431]

Najpre je potrebno izvršiti pripremne aktivnosti: reformatiranje, usklađivanje i čišćenje podataka. Ovde se mora naglasiti i činjenica nekompletnosti, nepreciznosti i nekonzistenstnosti podataka, dobijenih iz različitih datotetka i baza podataka. Ovi podaci zahtevaju unifikaciju , kako bi se u takvom formatu koristili u svim daljim fazama obrade. Čišćenjem se vrši uklanjanje onih podataka koji nisu od važnosti za dalju analizu.



Slika 39. *ETL proces*
Izvor: [431]

Neophodne promene u dizajnu sistema mogu prouzrokovati povećanja količine podataka. Veoma bitna karakteristika ETL sistema je skalabilnost koja se odnosi na razumevanje količine podataka koji će biti procesuirani. U cilju poboljšanja ukupnih performansi razvijaju se alati zasnovani na paralelnom procesuiranju. Osnovni tipovi paralelizma koji su intrepretirani u ETL aplikacijama su:

- *data* – deljenje posebne datoteke u manje datoteke podataka čime se obezbeđuje paralelni pristup,
- *pipeline* – mogućnost simultanog rada više komponenata na istom *data stream*-u,
- *component* – istovremeni rad višes procesa na različitom *data stream*-u u okviru istog posla.

Karakteristike standardnih ETL alata su takve da ukoliko imaju bolje performanse vezane za proces čišćenja podataka, onda im je slabiji kapacitet za procese transformacije ili obrnuto. Zato je pre izbora ETL alata potrebno poznavati karakteristike podataka koji će biti smeštani u skladište podataka. Pre same faze ekstrakcije podataka potrebno je definisati ciljane strukture podataka u koje će biti smešteni ekstrahovani podaci gde se najčešće koriste relacione baze podataka, kao i kombinacija različitih struktura. Implementacija prihvatnog područja u relacionoj bazi podataka je komplikovana, jer takva

struktura mora da iskazuje dobre performanse kako za unos velikih količina podataka tako i za njihov izvoz. [178]

6.9.3.5 Ekstrakcija podataka

Prvi korak u procesu integracije različitih izvora podataka predstavlja ekstrakcija podataka iz produkcionih sistema. Predstavlja prikupljanje podataka iz različitih izvora i platformi i smeštanje tih podataka u skladište podataka. Zapravo predstavlja selektivni proces unošenja informacija bitnih za odlučivanje u skladištu podataka. Proces ekstrakcije potrebno je realizovati sinhronizovano tako da što manje trpe redovni operativni poslovi. To je i razlog efikasnih ETL procese koji se mogu izvršavati uz nastojanje što bržeg zahvatanja potrebnih podataka iz operativnih procesa. Ovde se može pojaviti problem, potencijalno visoki stepen redundanse podataka u transakcionim sistemima. Zato je potreban izbor takvog pristupa ekstrakciji kojim će se vršiti zahvatanje onih podataka koji će se koristiti u aplikacijama poslovne inteligencije. [178]

Ovde se nameće osnovno pitanje kako pristupiti podacima u produkcionim sistemima, s obzirom na činjenicu da se oni mogu sastojati iz različitih sistema za upravljanje bazama podataka, operativnih sistema, hardvera, da koriste različite komunikacione protokole i sl. Izvlačenje podataka iz izvornih sistema u novo područje obično se vrši posebnim podsistemom za ekstrakciju podataka. Kada se podaci jednom premeste u prihvatno područje postaju nezavisni od izvornih sistema čime se otvara mogućnost za njihovu dalju transformaciju prema potrebama krajnjih korisnika.

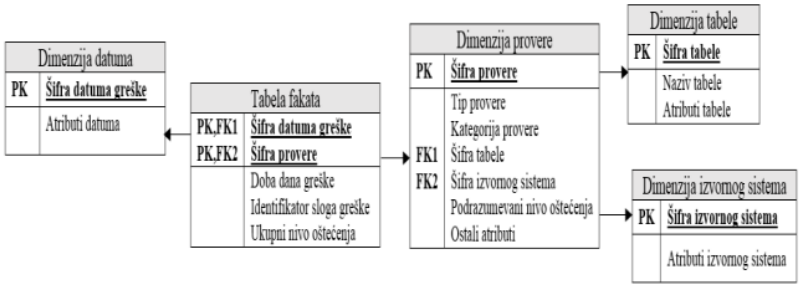
6.9.3.6 Proces transformacije podataka

Završetkom faze izvlačenja podataka smatra se da su podaci iz različitih izvornih sistema smešteni u određene strukture podataka samog ETL procesa. Najpre se vrši definisanje kvaliteta podataka, a nakon prolaska podataka kroz podsistem za transformaciju potrebno proverava se kvalitet podataka. Od podataka se očekuje da budu tačni, nedvosmisleni, konzistentni i kompletni.

Kvalitet podataka se definiše određenom politikom kvaliteta koju kreiraju krajnji korisnici, a koja zavisi od konkretne implementacije. Podsistem za transformaciju treba da bude u stanju da izvrši korekcije nad podacima u cilju popravke njihovog kvaliteta. Da bi što efikasnije realizovali popravke nad nekvalitetnim podacima, podsisteme za transformaciju delimo u četiri kategorije A, B, C i D:

- Kategorija A – podaci se ne mogu tehnološki generisati u podsistemu za transformaciju,
- Kategorija B – podaci koje bi trebalo popraviti na nivou izvornog sistema,
- Kategorija C – podaci koje treba srediti na nivou ETL pre nego na samom izvornom sistemu,
- Kategorija D – podaci koji se mogu popraviti isključivo na nivou ETL sistema.

Ispred sistema za transformaciju podataka, postavljaju se važni zadaci. Pre svega očekuje se da u identifikaciji grešaka, njihovom ispravljanju i dokumentovanju kvalitet informacija bude detaljan radi otkrivanja izvora nekvalitetnih podataka. Isto tako, očekuje se da sistem bude brz u obavljanju svog posla. [152]



Slika 40. *Zvezdasta šema za praćenje grešaka*
Izvor: [152]

Tabela događaja za praćenje grešaka (engl. *Error Event Table*) i skup odgovarajućih dimenzija je potreban u cilju praćenja kvaliteta podataka i identifikacije izvora loših poataka. Svaki podatak koji nema zadovoljavajući nivo kvaliteta, podsistem za transformaciju podataka beleži kao red u tabeli događaja za praćenje grešaka. Njena granularnost je na nivou pojedinačne greške. U tom pogledu pod greškom se smatra nekvalitetan podatak (slika 40). U cilju utvrđivanja kvaliteta podataka vrše se različite provere nad njim. Dimenzijom tabele opisane su tabele podataka koje definišu domen za datu proveru. Kroz dimenziju izvornog sistema opisan je izvorni sistem odakle je izvršena ekstrakcija podataka. Poslednje dve dimenzije služe za lociranje izvora nekvalitetnih podataka. Tabela događaja zvezdaste šeme predstavlja ključni skup meta podataka za identifikaciju, analizu i kontrolu kvaliteta podataka, čiji je cilj unapređenje kvaliteta podataka tokom vremena.

Provere nad podacima mogu se kategorizovati na sledeći način:

- provera svojstava atributa,
- provera strukture podataka i
- provera poslovne logike.

Ukoliko se proveravama otkrije greška, ona se beleži u tabeli događaja za praćenje grešaka. Takođe, beleži se i nivo oštećenja podataka. Ukoliko je on visok i iznad određene vrednosti, greške se smatraju fatalnim i mogu da zaustave ceo ETL proces. U drugom slučaju, ETL proces se normalno nastavlja. U cilju postizanja boljih performansi, provere se paralelizuju.

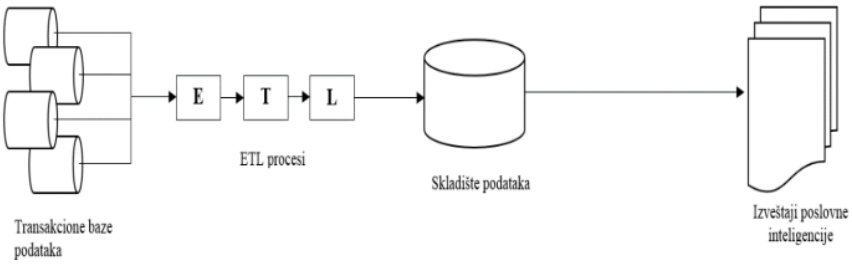
Nakon ovog koraka, po potrebi možemo nad njima izvršiti određene transformacije kako bi podaci bili ujednačeni i u skladu sa standardima. Važna karakteristika sistema za transformaciju podataka je otkrivanje duplikata. U nekim situacijama nije jednostavno pronaći duplikate te za tu namenu postoje specijalizovani alati koji se bave otkrivanjem duplikata i njihovim uklanjanjem. Nakon detekcije, duplikati se moraju objediniti u kvalitetan podatak koji je u skladu sa definisanom politikom kvaliteta podataka i koji će dalje biti prosleđen korisničkom području. U okviru ETL procesa najviše vremena se troši na postupak transformacije podataka, preko 80% od ukupnog ETL procesa. Možemo zaključiti da se u postupku transformacije mogu javiti različiti problemi koji usporavaju proces transformacije podataka, a najčešći se: [178]

- nekonzistentne vrednosti podataka,
- nepodudarnost primarnih ključeva koji se koriste u izvornim datotekama i bazama podataka koje pretpostavljaju aplikacije poslovne inteligencije,

- netačne vrednosti podataka,
- različiti formati podataka,
- problem sinonima i homonima,
- sakrivena procesna logika.

6.9.3.7 Proces punjenja skladišta podataka

U transakcionim sistemima, podaci se nalaze u bazama podataka koje obuhvataju kraće vremensko razdoblje tako da nisu dovoljni kao osnova za kvalitetne analize i podršku u odlučivanju. Deo izvornih podataka obrađenih ETL procesima čine i istorijski podaci. To implicira korišćenje više vrsta ETL programa za procese punjenja skladišta podataka kao što su programi za početno punjenje, punjenje istorijskih podataka i alati za dodavajuće punjenje. [432]



Slika 41. *Mesto i tok ETL procesa u kreiranju koncepta poslovne inteligencije*
Izvor: [432]

Alati za početno punjenje skladišta podataka je da sadrže procedure za čišćenje i usklađivanje podataka, kako bi se iz podataka uklonile greške. Na istorijske podatke ponekad nije moguće primeniti metode čišćenja koji se primenjuju za aktivne podatke, iz razloga mogućih različitih promena u slogovima i formatima podataka. Zato se za tu kategoriju podataka primenjuju programi za punjenje istorijskih podataka koji čine nastavak početnog punjenja. Za razliku od aktuelnih i ažuriranih podataka, istorijski podaci imaju statički karakter i čine samo sadržaj arhivskih datoteka. Treća vrsta su alati za dodavajuće dodatno punjenje podataka, a aktiviraju se nakon što su prethodna dva postupka realizovali čišćenje i usklađivanje podataka. Njihova karakteristika je da se pokreću periodično i oni predstavljaju stalno aktivan mehanizam punjenja skladišta podataka odgovarajućim sadržajima. Na slici 41, prikazan je tok ETL procesa u kreiranju skladišta podataka kao jednim od preduslova za razvijanje i primenu koncepta poslovne inteligencije.

6.9.3.8 Izbor arhitekture ETL sistema

Becker razmatrajući činioce donošenja odluke za primenu ETL arhitekture postavlja pitanje korišćenja komercijalnih alata ili razviti sopstveni ETL sistem. [433]

Prednosti komercijalnih ETL sistema su:

- prosto rukovanje, brži i jeftiniji razvoj,
- mogućnost korišćenja i lica koja nisu profesionalni programeri,
- sposobnost većine komercijalnih alata za automatsko generisanje potrebnih meta podataka ETL procesa,

- ugrađenost konektora za mnoge izvorne sisteme,
- dobre performanse,
- dobro upravljanje raspoređivanjem podataka u multiserverskim okruženjima (engl. *Loadbalancing*),
- fleksibilnost modularno napravljenih alata,
- razvijen sistem za dokumentovanje ETL procesa. [433]

Prednosti samostalno razvijanih ETL sistema su:

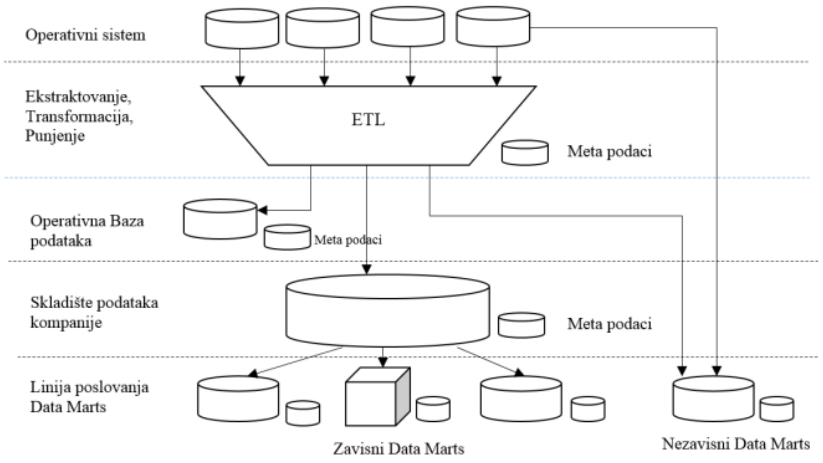
- upotreba alata za automatsko testiranje izgrađenog ETL sistema,
- potpuna fleksibilnost i nezavisnost od proizvođača softvera,
- sloboda u izboru struktura podataka potrebnih za ETL proces,
- očigledna manja inicijalna ulaganja u razvoj ETL sistema.

Najvažniji parametar u izboru ETL alata o kome treba posvetiti pažnju su potrebe kompanije. Potrebno je izabrati takav ETL sistem koji na najbolji mogući način može da odgovori na potrebe poslovnih korisnika i da njima najefektnije pruži potrebne informacije.

6.9.3.9 Osnovni modeli skladišta podataka

U praksi se sreću tri osnovna modela odnosno osnovne arhitekture skladišta podataka:

- dvoslojna arhitektura sa jednim zajedničkim skladištem podataka,
- dvoslojna arhitektura sa više nezavisnih lokalnih skladišta podataka (engl. *Data Mart*) i
- troslojna arhitektura sa zajedničkim skladištem podataka i više povezanih lokalnih skladišta podataka (slika 42).



Slika 42. *Troslojna arhitektura sa zajedničkim DW i više povezanih „Data Mart"*
Izvor: [172]

Pomoću *Data Mart* se pokriva jedna oblast poslovanja i može predstavljati pilot

projekat za realizaciju mnogo obimnijeg *Data Warehouse* sistema. Projekat može realizovati kao nezavisni *Data Mart*, gde je ETL sistem izolovan od *Data Warehouse* sistema, i kao zavisan *Data Mart*, naslonjen na *Data Warehouse* sistem.

6.9.3.10 Dvoslojna arhitektura sa zajedničkim skladištem podataka

Osnovna karakteristika ovog modela je jedinstveno i centralizovano skladište podataka. Podaci se zahvataju iz različitih izvora unutar kompanije i spoljašnjih izvora dostupnih putem Interneta ili nekim drugimnačinima.

Tabela 20. *Pregled Razlike između „Data Warehouse" i „Data Mart"*
Izvor: [168]

Osobina	*Data Warehouse*	*Data Mart*
Oblast	Poslovni sistemi	Sektor (org. celina)
Teme	Više	Jedna
Izvori	Više	Manji boj (nekoliko)
Tipična veličina	100 GB - > 1 TB	< 100 GB
Vreme implementacije	Meseci – godine	Meseci

Služi i većem broju organizacijskih celina kompanije kao i pojedinačnim korisnicima. Takva skladišta su obimna i veoma složena, sa ogromnim količinama podataka. Zato šeme podataka prema kojima se vrši skladištenje, treba da podržavaju široku lepezu aplikativnih zahteva. Iz navedenog možemo zaključiti da troškovi održavanja takve arhitekture postaju visoki i zahtevaju znatan angažman i vreme određenog broja i profila eksperata.

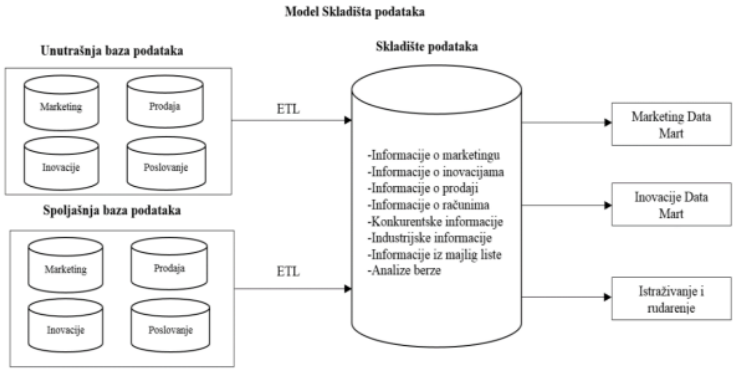
6.9.3.11 Dvoslojna arhitektura sa više nezavisnih lokalnih skladišta podataka

Ovu arhitekturu skladišta podataka karakteriše postojanje većeg broja nezavisnih lokalnih skladišta podataka sa namenom za rad pojedinačnih aplikacija prema organizacionim celinama kompanije. Osnovna odlika takve arhitekture se ogleda u velikom broju sistema u koji se posebno unose podaci iz različitih transakcionih baza podataka. Prednost ovakvog modela je u jednostavnosti izgradnje i lakoći korišćenja. Ipak, ovaj model ima i sledeće nedostatke:

- otežana komunikacija između organizacionih celina kompanije,
- paralelni rast i opterećenost transakcionih sistema povećanjem broja međusobno nezavisnih skladišta podataka,
- oblikovanost *data mart* tako da podržavaju samo jednu aplikaciju, pa problem predstavlja dodavanje novih aplikacija za određeno skladište,
- ograničena proširivost platforme,
- otežan uvid u stvarno stanje informacija na nivou kompanije.

6.9.3.12 Troslojna arhitektura skladišta podataka

Troslojnu arhitekturu skladišta podataka čini veći broj lokalnih skladišta podataka (engl. *data mart*) i jedno centralno skladište podataka (engl. *data warehouse*) koje se nalazi između skladišta podataka i različitih izvora podataka unutar i van kompanije. Baziraju svoj rad na radu centralnog skladišta koje im daje podatke u obliku koji pruža ujednačen uvid u sve segmente poslovanja kompanije (slika 43).



Slika 43. *Troslojni model sistema skladištenja podataka*
Izvor: [172]

Prednosti troslojne arhitekture se ogledaju u većoj tačnosti informacija nevezano za izvor podataka, olakšana komunikacija između organizacionih celina, smanjena opterećenost administratora, povećana skalabilnost i proširivost platforme za skladištenje podataka, kao i mogućnost korišćenja spoljnih aplikacija čime se obezbeđuje povezivanje svih subjekata unutar kompanije.

6.9.3.13 Implementacija skladišta podataka u poslovne subjekte

Implementacija i razvoj sistema skladišta podataka zahteva vreme i značajna finansijska sredstva. Međutim, uspešne kompanije se odlučuju na korišćenje ove tehnologije zbog činjenice da kompanije dobijaju mogućnost za brze reakcije na stanja nastala na tržištu, čime obezbeđuju uspešno poslovanje i opstanak na tržištu.

Postepena izgradnja sistema uz sukcesivno nadograđivanje jedan je od praktičnih pristupa. Primenom ovog pristupa u završnom koraku vrši se kreiranje troslojnog modela sistema skladišta podataka. Razvojem nekoliko skladišta podataka koja podržavaju troslojnu arhitekturu započinje postupak kreiranja ovog sistema. Nakon određenog vremena, posle razvijanja skladišta podataka, započinje se sa izgradnjom centralnog skladišta uz odvajanje pojedinih. Postupak izgradnje sistema skladišta podataka sastoji se iz nekoliko faza: [178]

- Definisanje zajedničkih elemenata svih predmetnih oblasti koje ima smisla ugraditi u svako lokalno skladište podataka.
- Razvijanje prve pilot-aplikacije kojoj se pridružuje skladište podataka podeljeno na dve komponente: na mini skladište i na skladište podataka.
- Tokom treće faze vrši se postepeno aktiviranje novih skladišta podataka i razvijanje novih aplikacija potrebnih za zahvatanje informacija iz mini skladišta razvijenog sa prvim skladištem.
- Četvrta faza podrazumeva odvajanja centralnog skladišta podataka čime se završava proces kreiranja troslojnog modela.

Uvođenjem i aktiviranjem ovog sistema u kompaniji pojaviće se novi zahtevi, pitanja i zadaci koje će zahtevati rešenje. Tada se javlja potreba za nadogradnjom ili modifikacijom sistema za transakcionu obradu podataka ili potreba za razvojem sistema koji će biti namenjen za zahvatanje podataka koji nedostaju. Važno je prilikom projektovanja skladišta podataka, korisnicima skladišta korisnicima postaviti pitanje koje

informacije će im biti potrebne posle implementacije novog *Data Warehouse* sistema. Mnogi krajnji korisnici skladišta podataka, koji su prošli edukaciju i koji su obučeni za njegovo korišćenje, nikad u potpunosti ne koriste sve mogućnosti koje im skladište pruža.[434]

6.9.3.14 Višedimenzionalni prikaz podataka

ETL postupkom, dobijaju se osnovni podaci skladišta. Primenom sistema za menadžment podataka generišu se multidimenzionalni podaci koji različitim analitičkim metodama obrade u procesu donošenja odluka omogućavaju dobijanje različitih oblika informacija potrebnih kompaniji. Najveća prednost dimenzione strukture je mogućnost vizuelne reprezentacije informacija. Kada se skladišta podataka povežu sa korisničkim interfejsom i odrede načini postavljanja upita i prikaza rezultata upita, menadžerima se omogućava jednostavno i brzo postavljanje upita kao i odgovarajući prikaz rezultata upita (tekst, slika, grafički prikazi i sl.).

Skladišta podataka podrazumevaju korišćenje dimenzione strukture podataka koja se zasniva na relacionim tabelama. U OLAP sistemima kao skladištima podataka koristi se multidimenzionalnost i denormalizacija. Vezni elemenat koji objedinjava sve elemente je centralna relaciona tabela. Ona smešta elemente primarnih šifri svake od relacionih tabela koje učestvuju u strukturi zajedno sa numeričkim varijablama čija je analiza potrebna. Skup OLAP alata služi za izvođenje znanja iz određenih skladišta podataka. Ključna karakteristika OLAP alata je multidimenzionalnost, tj. obezbeđivanja mogućnosti korisniku za analizu u različitim dimenzijama.

Zahtevi koje OLAP mora su: [435]

- rad sa velikim grupama podataka i velikim brojem korisnika,
- kratko vreme odziva na upit,
- rad sa podacima različitih nivoa detalja,
- sposobnost proračunavanja složenih matematičkih funkcija,
- podrška za *what-if* analizu, modelovanje i planiranje,
- jednostavnost implementacije i održavanja sistema,
- zaštita podataka,
- rad sa velikim brojem alata za pristup podacima, analizu i prikazivanje podataka.

Tabela 21. *Prikaz OLAP arhitektura i njihovih razlika*
Izvor: [435]

Arhitektura	Razlike	Prednosti	Nedostaci
ROLAP	izračunavanja u relacionim bazama podataka, veliki kapaciteti podataka	analiza velike količine podataka, korišćenje funkcionalnosti sistema relacionih baza podataka	izvođenje može biti loše zavisno od količine podataka, otežana primena standardnih upitnih jezika
MOLAP	izračunavanja u server baziranim multidimenzionalnim bazama podataka, kocke pružaju pristup za unos proračunskih podataka i obavljanje *what-if* analiza	odlično izvođenje zbog korišćenja multidimenzionalnih OLAP kocki, brz pristup podacima, primenjivost složenih izračunavanja	prilikom izračunavanja nije moguće obuhvatiti velike količine podataka jer se one moraju agregovati, zauzimanje prostora prilikom velikog broja dimenzija
HOLAP	sakupljanje u *cache,* ali pristupanje podacima pomoću *drill-through* procedura	koristi funkcionalnosti ROLAP i MOLAP arhitekture, velike brzine pristupa, relativno malo zauzimanje prostora	spor kao ROLAP kada pokušate pristupiti *leaf-level* podacima, treba preraditi sve prilikom unosa novih podataka
DOLAP	klijent bazirane, mini *cache* izgrađen prilikom *run-time* upita	*user-frinedly*, odlične performanse upita, najlakše za razviti i koristan mobilnim korisnicima koji se ne mogu često spajati na skladište podataka	ograničene funkcionalnosti i kapacitet podataka koje može spremiti

Razlikujemo sledeće arhitekture OLAP sistema:

Relacioni OLAP alati (engl. *Relational Online Analytical Processing, ROLAP*) sve dobijene podatke skladište u standardne sisteme relacionih baza podataka, tako da ne skladište ništa u eksterne repozitorijume. Sposobni su za rad sa velikom grupom podataka, što ih čini kompleksnim i skupim za implementaciju, a takođe imaju loše performanse izvršavanja upita tako da nisu sposobni da izvode složenije finansijske kalkulacije. Oni nužno ne skladište podatke za analizu odvojeno od ostalih izvornih podataka. Takođe, imaju otežanu primenu standardnih upitnih jezika (npr. *SQL*-a), pa korisnici neke druge oblike interakcije sa bazama podataka ne smatraju prednošću već nedostatkom. [436]

Multidimenzioni OLAP (engl. *Miltidimensional Online Anlytical Processing, MOLAP*) predstavlja alate kod kojih se podaci smeštaju u multidimenzionalne kocke, što onemogućava njihovo korišćenje u bazama podataka, pa su većinom podaci skladišteni u sopstvene optimizovane baze podataka višedimenzionalne matrične strukture. Najveća prednost ovakve OLAP arhitekture je brzina, što od ovih alata zahteva visoke performanse, sofisticirane multidimenzionalne kalkulacije i funkcionalnosti. Ipak, baš zbog toga, mana ovih alata je zauzeće ogromnog prostora u slučaju postojanja većeg broja dimenzija. [432]

Desktop OLAP alati (engl. *Desktop Online Anlytical Processing, DOLAP*) su bazirani na klijenta tako da često koriste i relacione i multidimenzionalne baze podataka. U poređenju sa ostalim specijalizovanim OLAP proizvodima imaju limitirane funkcionalnosti, koje se ogledaju u činjenici da su prilagođene za personalne računare, a samim time zadovoljavaju potrebe pojedinačnih korisnika.

Hibridni OLAP (engl. *Hybrid Online Anlytical Processing, HOLAP*) – kombinuje tehniku skladištenja podataka ROLAP i MOLAP arhitekture. Neke podatke skladišti u

multidimenzionalne baze podataka, dok drugi deo podataka skladišti u relacione baze podataka čime koristi pogodnosti obe tehnike. Prvi deo podataka čuva u relacionoj bazi podataka i pristupa im pomoću *drill-through* procedura, dok abstrakt čuva u multidimenzionalnoj kocki, čime se postiže velika brzina pristupa i relativno malo zauzimanje prostora. [432]

Prednost višedimenzionalna struktura podataka (MOLAP sistema) ogleda se u odličnim performansama sistema kada se radi sa izračunatim podacima (agregacijama) i rudarenje (engl. *drill up, drill down, drill through*), unakrsno tabelovanje (engl. *cross tabulation*), selekcija, isecanje, izdvajanje i kombinovanje svih dimenzija (engl. *slice and dice requirement*), rotacija odnosno isticanje jedne dimenzije dok su druge u pozadini (engl. *pivoting*), prognoza, modelovanje, grafičko prikazivanje (engl. *charting*), statistič ke analize (engl. *trend, klaster*) i sl. Nedostatak višedimenzionalnih struktura podataka se ogleda u teškoći dodavanja novih dimenzija, kao i činjenici da se bilo koju analizu, prvo trebaju učitati podaci u višedimenzione strukture. Kako bi se kreirale agregacije i popunili podaci vrše se razni proračuni, što je vremenski zahtevno. Po završenom procesu, korisnik može započinje analizu.

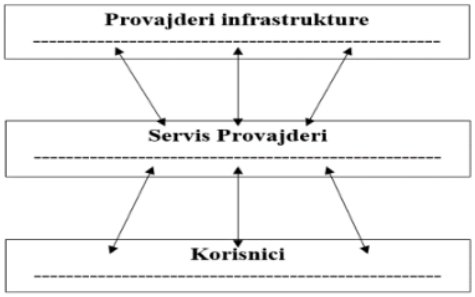
Tehnike otkrivanja znanja koje smo opisali omogućavaju kontinuirano pronalaženje novih informacija namenjenih za strateško, taktičko i operativno donošenje odluka u kompaniji. Primenom koncepta skladištenja podataka vrši se rasterećenje operativnih baza podataka od složenih upita, pa čitav informacioni sistem koji se sada sastoji od dva dela, operativnog i skladišta podataka postaje produktivniji i lakše se kontroliše i restrukturira.

6.9.4 Računarstvo u oblaku – *Cloud Computing* sistemi

Računarstvo u oblaku (engl. *Cloud Computing*) predstavlja tehnologiju u kojoj su grupe udaljenih servera umrežene u cilju pružanja centralizovanog čuvanja podataka i pristupa računarskim servisima ili resursima putem web-a. Zasniva se na deljenju resursa preko mreže. Predstavlja koncept objedinjene infrastrukture i deljenih servisa koji se orijentiše na maksimizaciju njihove efikasnosti. Ti resursi dele se na više korisnika i dinamički se raspoređuju na zahtev. Upotrebom *Cloud Computinga*, veliki broj korisnika može da pristupi jednom serveru kako bi preuzeo i ažurirao svoje podatke bez kupovine licenci za razl e aplikacije. Pruža mogućnost kompanijama da iznajme potrebnu infrastrukturu i hosting usluge umesto ulaganja u novu infrastrukturu, obuku kadrova ili licenciranja novog softvera. [437]

6.9.4.1 Definisanje računarstva u oblaku

Postoje različite definicije računarstva u oblaku. NIST [439] definiše računarstvo u oblaku kao „model koji omogućava jedinstven i precizan pristup na zahtev podeljenom pulu računarskih resursa koji mogu da se konfigurišu (kao što su mreže, server, storidži, aplikacije i usluge), mogu da se brzo realizuju i kojima se upravlja sa minimalnim resursima il a minimalnom interakcijom sa provajderima usluga...” Gartner ga definiše [440] kao „oblast računarstva u kojoj se skalabilni informatički kapaciteti pružaju u vidu usluge koja se putem interneta isporučuje brojnim eksternim potrošačima. [441] Forester je računarstvo u oblaku definisao kao „apstrahovanu, visoko skalabilnu i kontrolisanu računarsku infrastrukturu koja hostuje aplikacije namenjene krajnjim korisnicima i čije se usluge naplaćuju na bazi osnovne potrošnje”.[442]



Slika 44. *Osnovni model računarstva u oblaku („ Cloud Computing ")*
Izvor: [443]

Računarstvo u oblaku je rezultat evolucije i usvajanja postojećih tehnologija i paradigmi. Cilj računarstva u oblaku je omogućavanje korisnicima ostvarivanja koristi od tih tehnologija smanjivanjem troškova i pomoć korisnicima u fokusiraju na njihovu osnovnu delatnost.

6.9.4.2 Koncepti karakteristike računarstva u oblaku

Računarstvo u oblaku predstavlja novi koncept zasnovan na ranijim modelima distribuiranih usluga, u vidu uslužnog računarstva (engl. *utility computing*), usluge na zahtev (engl. *on-demand services*), mrežnog računartsva (engl. *grid computing*) usluge u vidu softvera (engl. *software-as-a-service*). U računarstvu u oblaku plaćaju se samo one usluge koje su potrebne korisnicima, ali se i u kratkom vremenskom roku može višestruko povećati njihov obim. [444]

Glavna tehnologija koja je omogućila računarstvo u oblaku je virtuelizacija. Uz virtuelizaciju na nivou operativnog sistema koja kreira skalabilni sistem više nezavisnih računarskih uređaja, računarski resursi mogu da budu alocirani i korišćeni mnogo efikasnije. Virtuelizacija obezbeđuje potrebnu agilnost da bi se ubrzale IT operacije i smanjili troškove povećanjem iskorišćenosti infrastrukture. Autonomno računarstvo automatizuje proces kroz koji korisnik može da pribavlja resurse na zahtev. Minimizovanjem uključenosti korisnika, automatizacija ubrzava proces, smanjuje radne troškove u umanjuje mogućnost ljudske greške. [445]

Karakteristike računarstva u oblaku su:

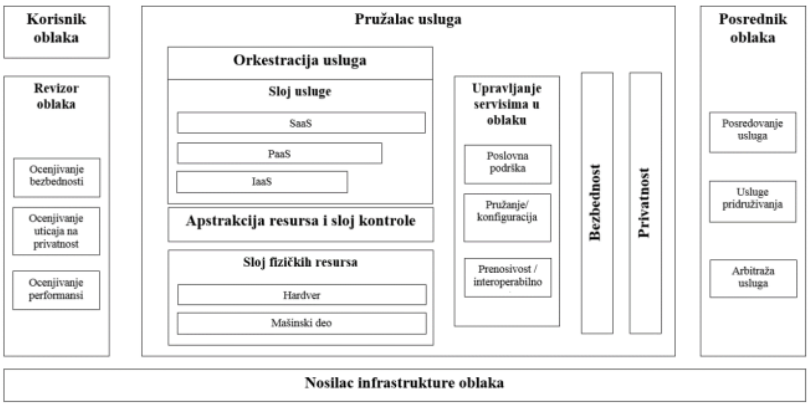
- masivna i apstraktna informatička struktura,
- dinamička alokacija, skaliranje i migracija aplikacija,
- plaćanje na osnovu utrošenih resursa (engl. *pay-per-use*), procesorskog vremena ili uz primenu modela reklamiranja,
- okruženje sa više paralelnih kompanija korisnika (engl. *multi-tenant environment*),
- aplikacije se koriste na zahtev (engl. *on-demand*),
- upravljački interfejs zasnovan na web-u
- mogućnost potpune samostalne kontrole korisnika u pogledu korišćenja i okončanja usluge. [446]

Uvođenje ove tehnologije nije prosto za kompanije, pa se najpre trebaju sagledati njeni nedostaci. Svaka kompanija prethodno treba da izvrši procenu finansijskih ušteda

koje će doneti korišćenje ovog modela i kako će se to odraziti na bezbednost i konkurentnost kompanije na tržištu. Tehnologija računarstvo u oblaku još uvek je u razvoju i neprekidno uvodi nove promene, pojavljuju se novi provajderi i sve više korisnika pristupa ovome konceptu na kome skladišti i čuva aplikacije.

6.9.4.3 Arhitektura računarstva u oblaku

Referentni model arhitekture računarstva u oblaku obuhvata generičke entitete koja identifikuje glavne uloge, njihove aktivnosti i funkcije u računarstvu u oblaku. [447] Osnovni model koji se danas najčešće primenjuje je davalac usluge i korisnik usluge koji su povezani putem Interneta. U tom slučaju korisnik zahteva uslugu direktno od davaoca usluge oblaka. [448]



Slika 45. *Referentna arhitektura računarstva u oblaku*
Izvor: [448]

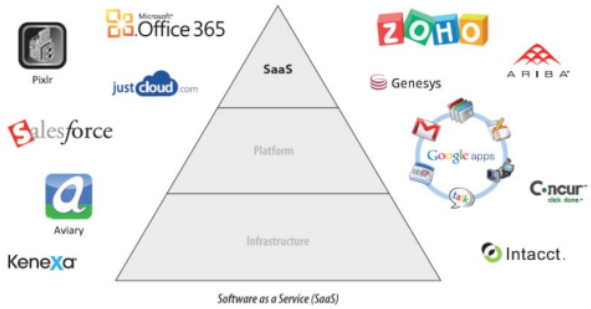
Na tržištu se javljaju i drugačije uloge, kao što su preprodavac/agregator usluga oblaka (engl. *cloud resseller/agregator*), prodavac programske podrške/usluga oblaka (engl. *cloud software/service vendor*), davalac alata za rad u oblaku (engl. *cloud tool provider*) i druge. Takođe, neki davalac usluge oblaka će delovati istovremeno i kao potrošač usluge, odnosno kao *Cloud Prosumer*.

Referentnu arhitekturu računarstva u oblaku čini pet činilaca: korisnik usluga oblaka, davalac usluga, nosilac infrastrukture, revizor i posrednik (slika 45). Svaki učesnik je subjekat (fizičko lice ili kompanija) koji učestvuje u transkaciji ili procesu i/ili izvodi zadatak u računarstvu u oblaku. [447] Korisnik oblaka je glavni učesnik koji realizuje poslovne odnose i koji koristi servise od davaoca usluga oblaka. On pregleda listu servisa davaoca usluga oblaka, potražuje prikladan servis, pravi ugovore servisa sa davaocem usluga i koristi servis. Njemu se naplaćuje davanje usluga. Davalac usluga je lice ili kompanija koja je zadužena za pružanje usluga korisnicima. Prikuplja i upravlja računarskim infrastrukturama koje su potrebne za pružanje usluga. [447] Revizor oblaka vrši nezavisno ispitivanje usluga kontrole oblaka. On ocenjuje bezbednosne kontrole, uticaj na privatnost, izvršavanje i slično. [447] Korisnik oblaka može zatražiti usluge oblaka od posrednika umesto direktnog kontaktiranja davaoca usluga. Preko posrednika se upravlja korišćenjem, izvršavanjem i isporukom usluga za oblak i pregovara o odnosima između davaoca usluga i korisnika oblaka. [447] Nosilac infrastrukture oblaka pruža servise oblaka od davaoca usluga do korisnika. [447]

6.9.4.4 Modeli usluga računarstva u oblaku

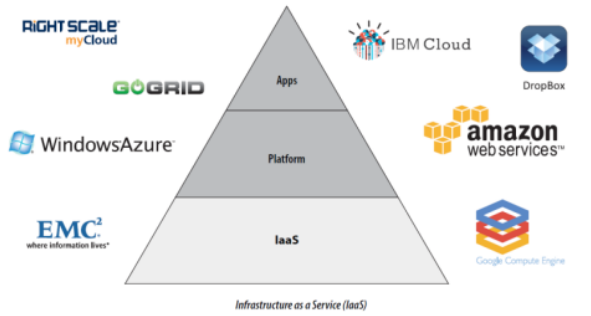
U računarstvu u oblaku se koristi model isporuke servisa SPI (engl. *Software*

Platform Infrastructure, *SPI*) koji označava tri najveće grupe servisa koji se pružaju putem oblaka. To su: Softver-kao-Servis (engl. *Software-as-a-Service, SaaS*), Platforma-kao-Servis (engl. *Platform-as-a-Service, PaaS*) i Infrastruktura-kao-Servis (engl. *Infrastructure-as-a-Service, IaaS*). [449] Na osnovu zahteva korisnika se isporučuju hardverski resursi. Svaki sloj arhitekture se može implementirati kao servis sloja koji se nalazi iznad. Slično tome, svaki sloj se može posmatrati kao korisnik sloja koji se nalazi ispod njega.



Slika 46. *Primer SaaS provajdera i aplikacija računarstva u oblaku*
Izvor: [450]

U modelu Softver kao servis – SaaS korisnik iznajmljuje softver od strane proizvođača a nalazi se u njegovom data centru i obezbeđuje pristup sistemu preko Interneta na bazi template. Pristup servisu se obavlja preko bilo kog uređaja. U tom smislu se razlikuju dva modela: prvi je klasični, licencni softver, koji radi na web serveru, a koji vlasnik softvera instalira, implementira i održava, dok drugi model predstavlja hostovano rešenje. [450] Model softvera kao servisa je namenjen za uobičajene radne funkcije kao što su: e-pošta (*Microsoft Exchange mail*) i desktop aplikacije (*Microsoft Word, Excel*). Pogodan je i za specifične funkcije kao što su računovodstvo i upravljanje odnosima sa klijentima (CRM). SaaS je najpoznatija i najkorišćenija kategorija, a pimeri *SaaS* su *Google Apps* i *Zoho Office*. [179]

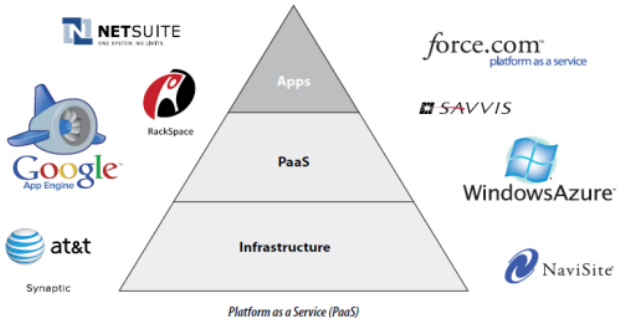


Slika 47. *Primer „IaaS" provajdera i aplikacija računarstva u oblaku*
Izvor: [450]

Kod modela Infrastruktura-kao-Servis (*IaaS*) iskorišćava se infrastruktura na bazi virtuelnih ili fizičkih resursa od strane korisnika. Korisnici plaćaju korišćenje usluge na osnovu ostvarene potrošnje (*pay-per-use*) sa mogućnošću da postave svoju aplikaciju na vrhu resursa koji se hostuju i mogućnošću upravljanja u data centrima vlasnika oblaka. Potrošač ima kontrolu nad operativnim sistemom, smeštajnim kapacitetima i aplikacijama

koje mu pripadaju, i ograničenu kontrolu nad izabranim mrežnim elementima. Vodeća kompanija koja obezbeđuje *IaaS* rešenja je Amazon, putem usluge *Elastic Compute Cloud* (EC2). U okviru njega se pruža velika računarska infrastruktura i servisi na bazi virtuelizacije hardvera.

Model Platforma kao servis (*PaaS*) pruža aplikacije ili prilagođenu platformu gde korisnici sami kreiraju aplikacije koje će koristiti u oblaku bez potrebe za prethodnom instalacijom odgovarajućih alata. Korisnik upravlja aplikacijama koje pokreće u tom okruženju, ima određena prava korišćenja, bez potpunih prava nad operativnim sistemom, mrežom, ili hardverom koji ta aplikacija koristi. Primeri *PaaS* modela su *Google App Engine*, *Microsoft Azure Services*, kao i *Force.com* platforma.



Slika 48. *Primer „PaaS" provajdera i aplikacija računarstva u oblaku*
Izvor: [450]

Sistemske komponente davaoca usluga oblaka koje su potrebne za stvaranje i isporuku usluga organizovane su u tri sloja: uslužni sloj (engl. *service layer*) koji sadrži mogućnosti za *SaaS*, *CaaS*, *PaaS*, *IaaS* i *NaaS* koje se na zahtev stavlja na raspolaganje korisniku; sloj apstrakcije i upravljanja (engl. *resource abstraction and control layer*) koji upravlja pristupom fizičkim resursima putem programske apstrakcije (virtuelna mašina, virtuelno skladište, virtuelna mreža…) i sloj fizičkih resursa (engl. *physical resource layer*) koji sadrži računarske i komunikacione resurse. [448]

Za telekomunikacione usmerene računarske oblake ITU-T Fokus grupa računarstva u oblaku [451] predlaže još dva dodatna modela: komunikacija kao usluga (engl. *Communications as a Service, CaaS*) i mreža kao usluga (engl. *Network as a Service, NaaS*).

6.9.4.5 Modeli implementacije računarstva u oblaku

Postoje četiri različita razvojna modela prema kojima se pružaju usluge *cloud computing*. [452] Zavisno od specifičnosti potreba ta četiri modela izvedena su na četiri različita načina: [453]

- javni (eksterni) *cloud*,
- privatni (interni) *cloud*,
- *cloud* zajednice (engl. *community cloud*) i
- hibridni *cloud* [454].

Javni oblak (engl. *Public Cloud*) predstavlja model kod koga pružaoci servisa obezbeđuju javni pristup svojim resursima. Obezbeđuju niz pogodnosti za pružaoce servisa, koji se ogledaju u tome da nema potrebe za ulaganjem u infrastrukturu, pomerajući

na taj način rizid od ulaganja ka provajderima infrastrukture. On je prepušten kompaniji koja nudi usluge tehnologije oblaka brojnim korisnicima preko zajednicke infrastrukture. To je inače trenutno najčešce korišćena vrsta oblaka. Smatra se da su resursi u javnom oblaku neograničeni. Održavanje se prepušta distributerima oblaka koji utiču na politiku servisa, cene, profit i modele naplate. Njihov glavni nedostatak je smanjena bezbednost informacija i kontrole nad podacima i mrežom, što može dovesti do umanjenja efikasnosti u nekim modelima poslovanja. [455]

U privatnom oblaku (engl. *Private Cloud*) jedan korisnik ima ekskluzivno pravo korišćenja, sa maksimalnom kontrolom nad podacima, bezbednošću, pouzdanošću i kvalitetom usluga. Kompanija ima u posedu kompletnu infrastrukturu, i kontrolu nad aplikacijama koje se isporučuju u privatnom oblaku. Motivacija da se formira privatni oblak u okviru neke kompanije pored optimizacije resursa je i aspekt bezbednosti i privatnosti informacija. [456]

Oblak zajednice (engl. *Community Cloud*) predstavlja strukturu oblaka koju deli nekoliko organizacija. Infrastruktura oblaka zajednice (oblik javnog oblaka pod kontrolom) isporučuje specifičnu uslugu unutar neke organizacione celine prema prethodno definisanim zahtevima. Organizacija ili davaoc usluge upravlja resursima oblaka. Prednost mu je što se troškovi mogu deliti između klijenata. [457]

Hibridni oblak (engl. *Hybrid Cloud*) predstavlja kombinaciju istrovremenog korišćenja i javnog i privatnog oblaka čime se pokušava prevazići ograničenja oba modela. Tako se optimizuje bezbednost i privatnost uz smanjene IKT investicije. Bezbednosno osetljiv deo servisne infrastrukture ostaje u privatnom, dok se drugi deo nalazi u hibridnom oblaku. Hibridni oblaci su fleksibilniji i omogućavaju bolju kontrolu i bezbednost nad aplikacijama u poređenju sa javnim oblacima, zadržavajući pri tome mogućnost njihove nadogradnje.

6.9.4.6 Problemi i rizici bezbednosti računarstva u oblaku

Korisnik koji razmišlja, pre izbora kompanije čiju će uslugu oblaka koristiti, najpre treba da izvrši procenu bezbednosti korišćenja ove tehnologije. Procena bezbednosti se najbolje može izvršiti od strane eksperata u ovoj oblasti. U područjima kao što su inovacija, usklađenosti kontrole i revizija računarstva u oblaku zahteva i procenu pravnih problema. Korisnicima se mora obezbediti transparentnost i treba da izbegavaju pružaoce usluga koji odbijaju da daju detaljne informacije o bezbednosnim problemima. Takođe, korisnici moraju biti upoznati sa sposobnostima onih koji vode politiku kompanije, arhitektama, programerima i operaterima, procesima kontrole rizika i tehničkih mehanizama, sprovedenom nivou testiranja kako bi se potvrdilo da procesi kontrole i usluge rade na planiran način, ali i o tome da li su davaoci usluga sposobni da identifikuju neočekivane ranjivosti.

Neki od karakterističnih bezbednosnih rizika su: [458]

- zavisnost od provajdera i usluga,
- gubitak upravljanja i kontrole,
- izolacija resursa,
- rizik saglasnosti,
- rizik pristupa resursima,
- zaštita podataka,

- nebezbedno ili nepotpuno brisanje podataka,
- zlonamerni insajderi.

Uobičajeni bezbednosni zahtevi za računarstvo u oblaku su: poverljivost, integritet, dostupnost i neporečivost.

Kako bi se postigao zadovoljavajući stepen bezbednosti, ali i koordinacije i međusobne povezanosti između korisnika i provajdera postoje standardi. Te standarde postavljaju grupe i organizacije. To su: *Cloud Security Alliance (CSA), Cloud Standards Customer Council (CSCC), Distributed Management Task Force (DMTF), IEEE Standards Association (IEEE-SA), National Institute of Standards and Technology (NIST), Organization for the Advancement of Structured Information Standards (OASIS), Storage Networking Industries Association (SNIA)*. [450] Njihov zadatak je promovisanje primera dobre prakse poznatih kompanija radi obezbeđivanja većeg stepena bezbednosti u okruženju računarstva u oblaku.

6.9.4.7 Prednosti i nedostaci računarstva u oblaku

Osnovne prednosti računarstva u oblaku su: [459][460]

- upotreba servisa na zahtev,
- dostupnost servisa,
- mrežni pristup,
- grupisanje resursa,
- elastičnost resursa,
- kvalitet usluge (QoS),
- merljivost usluga,
- bezbednost,
- skalabilnost. [453]

Najvažniji nedostaci računarstva u oblaku su dostupnost i bezbednost. [461] Međutim, u praksi postoje i još neki određeni nedostaci:

- problem zavisnosti od jednog provajdera programske podrške,
- implementacija novog načina razvoja aplikacija,
- nemogućnost jednostavnog premeštanja postojećih aplikacija
- odsustvo standarda za povezivanje aplikacija različitih proizvođača, razmenu podataka, premeštanje podataka kao i programske podrške iz „oblaka jednog proizvođača" u „oblak drugog",
- izostanak jasnoće u pogledu licenciranja,
- sistem upravljanja digitalnim identitetima i pristupom,
- poštovanje propisa postaje složenije.

Eksperti za bezbednost računarstva u oblaku intenzivno rade na smanjenju nedostataka koji su se do sada pojavili, pa analitičari smatraju da će najveći problemi biti rešeni. To će sigurno doprineti još većoj upotrebi računarstva u oblaku.

6.9.5 Hadoop sistemi

Hadoop sistem predstavlja programsko okruženje otvorenog koda (engl. *open-source framework*) koji funkcioniše pod pokroviteljstvom *Apache Software* Fondacije. Hadoop je *Apache* projekat, napisan u Javi i sastoji se računarskim okruženjem ili ekosistemom koji je baziran na *HDFS* (engl. *Hadoop Distributed File System, HDFS*) namenjenog za skladištenje podataka i *MapReduce* namenjenog za obradu podataka. [462]

Zbog mogućnosti pokretanja raznih upita i operacija nad podacima Hadoop predstavlja jeftino rešenje za skladištenje velike količine podataka. Pruža veliki kapacitet za sve vrste podataka, široke mogućnosti procesuiranja, kao i mogućnosti podrške neograničenih paralelnih zadataka. Omogućava rastavljanje većih problema na manje u cilju brze i jeftine analize. [463]

Poznate kompanije korisnici Hadoop modula su: *Cloudera, Hortonworks, IBM, Pentaho, Fico, Jaspersoft, Apache Bigtop, Cascading, Amazon Elastic MapReduce, Azure HDInsight* i drugi. Apache Hadoop prate tri ključna trenda: prelazak na skalabilnu i elastičnu infrastrukturu; kompleksna i raznolika struktura dostupnih podataka; snaga i vrednost koje dolaze iz kombinovanja različitih podataka za obavljanje sveobuhvatne analize. [464]

6.9.5.1 Bazne komponente Hadoop platforme

Hadoop predstavlja skup tehnologija koji je namenjen za skladištenje i obradu velikih količina podataka. U osnovi se Hadoop sastoji od HDFS-a (engl. *Hadoop Distributed File System, HDFS*) kao baze za skladištenje podataka i *MapReduce*-a koji predstavlja interfejs za obradu velikih količina podataka uskladištenih u HDFS. Hadoop omogućava izvršavanje aplikacija zasnovanih na *MapReduce* sistemu na velikom broju klastera običnog hardvera. Dizajniran je tako da paralelizuje obradu podataka primenom čvorova za povećanje brzine izračunavanja i smanjivanje odziva.

Hadoop čine četiri glavne komponente: [465]

- *Hadoop Common* paket,
- Hadoop distributivni sistem datoteka (*HDFS*),
- *Hadoop MapReduce* i
- *Hadoop YARN*.



Slika 49. *Pregled Hadoop okruženja i eko-sistema*
Izvor: [314]

Hadoop Common paket uključuje potrebne Java arhive odnosno *JAR* datoteke i skripte koje su potrebne za pokretanje Hadoop-a. On sadrži izvorni kod i dokumentaciju i sve potrebne elemente za komunikaciju Hadoop-a sa ostalim alatima. Struktura paketa je promenjiva s obzirom na predstavljanje novih verzija.

Clusteri su naziv za grupu koja se sastoji od dva ili više računara koja su povezana brzom mrežom. Ti računari nazivaju se čvorovi (engl. *nodes*) ili domaćini (engl. *hosts*), a u Hadoop, čvorovi mogu biti klasifikovani kao glavni (engl. *master*) ili radni (engl. *worker*) čvorovi. *NameNode* predstavlja glavni čvor koji kontroliše Hadoop sistem kroz dva podsistema, HDFS i sistem za upravljanje i alokaciju resursa *YARN* (engl. *Yet Another Resource Negotiator, YARN*) kao još jedan pregovarač resursa.[466]

Hadoop distributivni sistem datoteka HDFS zasniva se na *Google File* sistemu. Predstavlja sistem u kome je definisano kako se podaci skladište, kopiraju i čitaju.[462] Omogućava da se podaci distribuiraju u grupe kako bi se iskoristila mogućnost njihove paralelne obrade uz pomoć *MapReduca*. Svaka datoteka deli se u blokove čija veličine zavisi od našeg izbora. Takođe, HDFS skladišti (čuva) tri kopije svakog bloka u slučaju da se dogodi neka greška ili se neki računar pokvari.[467] Sve što se obrađuje uz pomoć Hadoopa treba biti uvezeno u HDFS gde će biti skladišteno na računarsku mrežu.[468] Za upravljanje pristupom podataka, HDFS koristi tri *Java daemona* (pozadinska procesa):

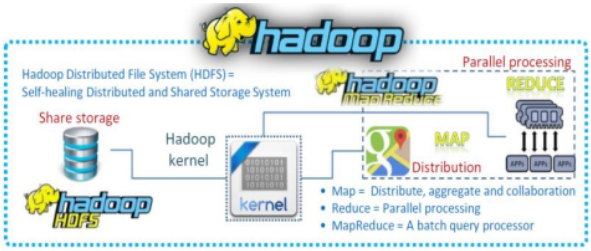
- *NameNode* – odlučuje i prati gde su se razni blokovi podataka skladištili.
- *DataNode* – upravlja skladištenim podacima na mašinama.
- *Secondary DataNode* – omogućava da se izvrši deo posla koji

odrađuje *NameNode*.[467]

MapReduce predstavlja rešenje efikasnog izvođenja skupa funkcija nad velikim količinama podataka na serijski način. To je programski model za obradu velikih količina podataka čiji se algoritam izvršava paralelno i raspodeljeno. [470] Može se posmatrati kao dva odvojena dela, *Map* deo i *Reduce* deo. Komponenta *Map* je zadužena za

raspoređivanje programerskog problema ili zadataka na veliki broj sistema i upravlja postavljanju zadataka na način koji podrazumeva balansiranje opterećenje i upravlja oporavkom od grešaka. Po završetku distribuirane obrade, poziva se druga funkcija *Reduce*, koja spaja sve elemente nazad zajedno, kako bi obezbedila rezultat.

U kombinaciji sa *HDFS*-om *MapReduce* dolazi do maksimalnog izražaja. *DateNode* skladišti podatke a *NameNode* se č[illegible] meta podatke o njima. Podelom podataka u blokove, olakšava se njihova obrada, što je skladištenje p[illegible]ataka u blokove olakšalo *Map* funkciji da ih grupiše. Svaki čvor može da izvršava ili *Map* ili *Reduce* zadatke, a s obzirom da svaki podatkovni čvor sadrži više podataka, moguće je očekivati izvršavanje zadataka u isto vreme za različite blokove poda[illegible]a. Pored njih, bitnu ulogu imaju: *JobTracker* koji vrši komunikaciju sa *NameNode* kako bi dodelio *MapReduce* zadatke određenom čvoru unutar računarskih direktorijuma i *TaskTracker* koji pokreće i prati odvijanje *MapReduce* zadataka u računarskim direktorijumima; kontaktira *JobTracker* u vezi dodeljenih zadataka i ako se određeni zadatak ne izvrši, njegov status šalje *JobTracker*-u koji taj isti zadatak dodeljuje neko novom čvoru unutar računarskih direktorijuma. Pomoću *MapReduce* sistema se upravlja distribuiranim serverima i generalno celim procesom. Sistem izvršava različite zadatke paralelno, upravlja svim komunikacijama kao i prenosu podataka između različitih delova sistema, u isto vreme obezbeđuju sistem od redundantnosti i grešaka.



Slika 50. *Prikaz Hadoop kernel*
Izvor: [314]

Hadoop YARN (engl. *Yet Another Resource Negotiator, YARN*) predstavlja novu komponentu u drugoj generaciji Hadoop-a sa ciljem da se *MapReduce* razdvoji u dva dela radi olakšanog korišćenja čitave platforme. [471] Osnovna namena *YARN*-a je upravljanje resursima u računarskim direktorijumima. Sastoji se od dve komponente: *Scheduler* i *Applications Manager* koje zajedno čine *Resource Manager*. Još jedna mogućnost koja se [illegible]ila sa *YARN*, je i mogućnost pokretanja većeg broj aplikacija koje su pisane za Hadoop. *Scheduler* je komponenta koja brine o alokaciji [illegible]ursa aplikacijama koje se izvršavaju. Obzirom da je alokacija resursa glavna aktivnost, ne vodi se računa o tome da li je došlo do greške ili je kod nekvalitetan, što implicira da će resursi biti dodeljeni aplikaciji dokle god se njen rad ne prekine od strane korisnika ili neke druge komponente. *Applications Manager* upravlja aplikacijama pisanim za Hadoop. Njegov zadatak je u pregovaranju i prihvatanju poslova. Pod pregovaranjem se [illegible]odrazumeva ispitivanje resursa i donošenje zaključaka što je prvi zadatak. Takođe, zadužen je i za resetovanje posla, odnosno aplikacije ukoliko dođe do neke greške.

Popularnost Hadoop rezultirala je razvojem besplatnih i plaćenih alata kako bi se olakšalo korištenje ili dodalo još funkcija. Najpopularniji su: *Pig*, *Hive*, *HbaseMahout*, *Hcatalog Ambari*, *Cassandra*, *Chukwa*, *Flume*, *O[illegible]e*, *Sqoop*, *Spark*, *Solr*, *Zookeeper* [467][468][472][473][474]. Moguć je izbor i nekog od komercijalnih distribucija Hadoop, a od kojih su poznatije *Cloudera*, *Hortonworks* i *MapR*.

Prilikom izbora Hadoop platforme treba imati u vidu da je to važna odluka koja ima dugotrajne posledice na čitavu kompaniju i to na način koji se u inicijalnom trenutku izbora platforme ne mogu predvideti. Sama infrastruktura Hadoop zahteva veliku opreznost pri konfiguraciji i izboru, kao i ostala oprema – serveri, skladištenje, baze podataka. Pored toga, na Hadoop utiču i razni ugovori o nivou pružanja usluge, zaštiti podataka, bezbednost, integracija sa ostalim aplikacijama, profesionalne usluge i trening. Važno je pronaći rešenje koje će se prilagoditi načinu poslovanja, umesto zahteva Hadoop tehnologije koja za određenu kompaniju nije primenjiva. [475]

6.9.5.2 Eko-sistem Hadoop

Hadoop eko-sistem predstavlja skup alata (projekata) koji zajedno rade na Hadoop platformi. Uz alate, *HDFS* i *MapReduce*tu su različiti *Apache* licencirani projekti, dok kompanije kao što su *Facebook* i *Microsoft* razvijaju svoja sopstvena rešenja. Izbor potrebnih projekata za rad i proces instalacije na personalnom računaru je danas olakšan obzirom da postoje kompanije koje pružaju Hadoop usluge sa izgrađenim eko-sistemom. Među najpoznatijim su: *Cloudera, Apache, MapR Technologies, IBM* i druge, ali najbolju platformu za početnike nudi besplatna *Hortonworks* platforma za podatke (engl. *Hortonworks Data Platform, HDP*). [462]

Osnovni alati (projekti) koji su dostupni na različitim platformama su:

- distribuirani sistemi datoteka *(HDFS)*,
- distribuirano programiranje *(MapReduce, Apache Pig, Apache Tez)*,
- NoSQL baze podataka *(Apache HBase, Apache Accumulo)*,
- SQL baze podataka *(Apache Hive, Apache HCatalog)*,
- unos podataka *(Apache Flume, Apache Sqoop, Apache Storm)*,
- programiranje usluga *(Apache Zookeeper)*,
- upravljanje podacima *(Apache Oozie, Apache Falcon)*,
- mašinsko učenje *(Apache Mahout)*,
- bezbednost *(Apache Knox)*,
- razvoj sistema *(engl. System Deployment Apache Ambari, HUE)*. [462]

6.9.5.3 Prednosti korišćenja Hadoop

Glavna prednost uvođenja Hadoop-a u poslovanje je njegova sposobnost skladištenja i obrade velike količine podataka bilo koje vrste velikom brzinom. Konstantnim povećanjem obima i izvora podataka sa društvenih mreža i Internet objekata, brzina obrade podataka postaje ključna osobina koja se uzima kao faktor. Ostale prednosti korišćenja Hadoop su: [463]

- računarska snaga,
- fleksibilnost,
- tolerisanje kvarova,
- niska cena,
- skalabilnost. [464]

7. Optimizacija zaštite memorije organizacije

Informacioni sistemi i memorija organizacije kao njen sastavni deo, izloženi su različitim vrstama bezbednosnih pretnji koje mogu prouzrokovati značajne finansijske gubitke i štete na resursima informacionog sistema, ali i kompanije u celini. Izvor tih pretnji mogu biti neželjene aktivnosti „pouzdanih" zaposlenih lica, hakerski napadi, slučajni propusti u unosu podataka i slično.[476] Narušavanje osnovnih načela informacionog sistema može imati negativne posledice za kompaniju. Zato se nameće potreba zaštite informacija, kao i upravljanja bezbednošću informacionog sistema kompanije kroz sveobuhvatan, detaljan i sistemski proces identifikovanja potreba, postizanja i održavanja zadovoljavajućeg nivoa bezbednosti informacionog sistema.[477]

7.1 Pretnje i ranjivosti memorije organizacije

Kada se razmatraju pretnje i ranjivosti memorija organizacije sami termini nemaju isto značenje. Pod pretnjom se smatra lice ili događaj koji mogu negativno uticati na vredan resurs. Ranjivost predstavlja osobinu resursa ili njegove okoline koja omogućava pretnju realizaciji. Razmatrajući različite kriterijume postoji veliki broj klasifikacija pretnji.

7.1.1 Bezbednosne pretnje

Bezbednosna pretnja može se razumeti kao događaj koji dovodi do povrede informacione poverljivosti, celovitosti i dostupnosti ali i bilo kog drugog oblika štete na resursima informacionog sistema. Posledice bezbednosne pretnje su različite, tako da neke bezbednosne pretnje utiču na poverljivost i pouzdanost sačuvanih podataka, a neke pretnje utiču na funkcionalnost i produktivnost čitavog informacionog sistema.

Memorija organizacije kao resurs kompanije izložena je raznim vrstama pretnji. Pretnja može da prouzrokuje neželjeni događaj tako da posledica može biti nanošenje štete memoriji organizacije. Pretnja mora da iskoristi postojeću ranjivost memorije organizacije kako bi se realizovala i rezultat bio nastanak štete u informacionom sistemu kompanije. Pretnje nastaju prirodnim putem ili ljudskim delovanjem (slučajne ili namerne).

Tabela 22. *Zajednički primeri pretnji*
Izvor: [459]

Ljudske		Prirodne
Namerne	**Slučajne**	
prisluškivanje	greške i propusti	zemljotres
modifikacija informacija	namerno brisanje datoteka, podataka i sl.	udar groma
„hakovanje"	pogrešno preusmeravanje	poplava
maliciozni kod	namerno fizičko uništenje	požar
krađa		

Pretnje dolaze iz različitih izvora, imaju različite uzroke i nepredvidive su. To je razlog zbog čega teško njihovo eliminisanje u potpunosti. Pretnja se može pojaviti unutar same kompanije ili izvan nje. Neželjeni događaji koji uzrokuju pretnje mogu biti prolazne prirode ili trajni (slučaji potpunog uništavanja resursa kompanije). Šteta uzrokovana nekom pretnjom može se razlikovati prema neželjenom događaju. Pretnje je često moguće

kvantifikovati i/ili kvalifikovati kako bi se ocenila njihova razorna moć. Neke pretnje mogu da utiču na više resursa kompanije tako da mogu imati različiti učinak u zavisnosti od resursa kompanije. Svaka pretnja ima određene karakteristike koje pružaju korisne informacije o samoj pretnji. Takve korisne informacije uključuju:

- izvor – da li je reč o unurašnjoj ili spoljašnjoj pretnji,
- motiv – ostvarivanje finansijske dobiti, ostvarivanje konkurentske prednosti,
- frekvencija pojavljivanja i
- razorna moć.

Pretnje je moguće opisati i deliti prema različitim kriterijumima. Tako ISO/IEC 17799 : 2000 prema vrsti njihovog izvora razlikuje sledeće bezbednosne pretnje: [478]

- prirodne katastrofe (zemljotresi, poplave, požari, oluje...),
- tehničke pretnje (tehnički problemi, kvarovi, komunikacione greške...),
- ljudi – nenamerne pretnje (nedisciplina, nemar, neadekvatan softver...),
- ljudi – namerne pretnje (sabotaža, diverzija, špijunaža, prevara, krađa, virusi).

Prema kriterijumu područja na koje je usmerena određena pretnja razlikujemo: [479]

- napade na fizičku bezbednost *(Ear tapping, DoS, Trash digging)*,
- napade na ličnu bezbednost (*User's password guessing, Masquerading (false identity), Social engineering, Extortions, Software piracy*),
- napade na komunikaciju i bezbednost podataka (*Attacks on data, Attacks on software*),
- napade na operativnu bezbednost (*Data frauds, Spoofing, Sniffing, Searching, Privileged access*).

Uticaj pretnji na sistem može se manifestovati kroz narušenost integriteta, dostupnosti i poverljivosti, koje obezbeđuje bezbednosna politika.

Integritet predstavlja zaštitu podataka od namerne ili slučajne neovlašćene izmene. Hakeri, lažno predstavljanje, neovlašćene aktivnosti i nedozvoljeni pristupi, kao i druge aktivnosti koje mogu dovesti do neovlašćenog menjanja podataka utiči na integritet podataka. Prvi korak u narušavanju dostupnosti ili poverljivosti sistema je najčešće povreda integriteta. Tri osnovna principa uspostavljanja kontrole integriteta su: [479]

- dodeljevanje samo nužnih prava pristupa (engl. *need-to-know basis*),
- odvajanje dužnosti i obaveza (engl. *separation of duties*),
- rotacija dužnosti (engl. *rotation of duties*).

Dostupnost podataka i informacija predstavlja garanciju dostupnosti sistema u svakom trenutku ovlašćenim korisnicima. Nedostupnost informacionog sistema potrebnog za izvršavanje svakodnevnih poslovnih zadataka u kompaniji može negativno da utiče na ciljeve kompanije i kontinuitet poslovanja. Dva su najčešća uzroka nedostupnosti sistema: [479]

- uskraćivanje usluge (engl. *Denial of Service, DoS*) i
- gubitak sposobnosti obrade podataka kao rezultat prirodnih nepogoda ili

ljudskih akcija.

Poverljivost predstavlja zaštitu podataka koja sadrži sistem bezbednosti od neovlašćenog pristupa koji se može narušiti na razne načine. Neovlašćeno, neočekivano ili nenamerno otkrivanje ili objavljivanje podataka može da dovede do gubitka poverljivosti sistema i podataka. Gubitak poverljivosti dalje implicira teže povrede važećih propisa i utiče na gubitak poverenja javnosti i narušavanja ugleda kompanije, što dalje prouzrokuje i pokreće pitanje sudskih procesa protiv kompanije. Najčešći načini narušavanja poverljivosti su:

- hakeri,
- lažno predstavljanje,
- nezaštićeno preuzimanje podataka i
- trojanski konji.

7.1.2 Procena ranjivosti

Ranjivost (engl. *vulnerability*) predstavlja eksploataciju slabosti sistema. Ranjivost predstavlja manu ili propust u bezbednosnim procedurama sistema, njegovom dizajnu, implementaciji ili unutrašnjim kontrolama koja može biti iskorišćena i rezultirati povredom bezbednosti. Identifikacijom ranjivosti informacionog sistema utvrđuju se moguće pretnje. Pored bezbednosne pretnje, ranjivost je drugi ključni kriterijum za procenjivanje verovatnoće bezbednosnih rizika, tako da je potrebno uvek sagledavati ih povezano. Određivanje stepena bezbednosnog rizika, a samim tim i adekvatne zaštite ključna je detaljna procena ranjivosti. S obzirom, da se okruženje kompanije i informacionog sistema može brzo promeniti, javlja se potreba za konstantnim praćenjem svih oblika ranjivosti u cilju izvršavanja identifikacije onih ranjivosti koje su postale izložene starim i novim pretnjama. Analizom ranjivosti vrši se procena slabosti koje identifikovane pretnje mogu iskoristiti. Ranjivost u odnosu na neku pretnju, pokazatelj je sa kojom će lakoćom neko ili nešto naneti štetu informacionom sistemu ili resursima kompanije. [480]

Informacije za određivanje ranjivosti prikupljaju se iz različitih izvora:

- razgovora sa odgovarajućim licima,
- pretraživanjem javnih baza o ranjivosti informacionih sistema,
- realizacijom specijalizovanih istraživanja ranjivosti,
- pregledom i ekspertizom bezbednosnih politika, sistemske dokumentacije i ostalih dokumenta koji se odnose na bezbednost,
- upotrebom alata za skeniranje sistema.

Tabela 23. *Tabela verovatnoće pretnje*
Izvor: [459]

Nivo verovatnoće	Definicija verovatnoće
Visoki	Pretnja je visoko motivisana i ima dovoljno mogućnosti za realizaciju, a kontrole koje bi trebale sprečiti iskorišćavanje ranjivosti su neefikasne.
Srednji	Pretnja je motivisana i ima mogućnost za realizaciju, ali postoje kontrole koje mogu sprečiti uspešno izvođenje pretnje.
Nizak	Pretnja nije motivisana ili nema dovoljno mogućnosti za realizaciju, ili postojanje kontrole koje mogu sprečiti iskorišćavanje ranjivosti.

Pored identifikacije ranjivosti važna je i procena verovatnoće realizacije ranjivosti, a pri tome se uzimaju u obzir:

- motivisanost i interes izvora,
- priroda ranjivosti i
- efikasnost sistema bezbednosti. [481]

7.1.3 Procena rizika

Bezbednosni zahtevi identifikuju se metodičkom procenom bezbednosnih rizika. Rezultati procene rizika predstavljaju jednu vrstu pomoći prilikom određivanja prioriteta i adekvatnih akcija kod upravljanja bezbednosnim rizicima. Procena rizika se mora sprovoditi periodično kako bi se u procenu uključile sve promene koje bi mogle uticati na rizik, implementaciju i održavanje sistema i sl. [482]

Tabela 24. *Matrica nivoa rizika* (engl. *Risk-Level Matrix*)
Izvor:[463]

Verovatnoća da izvor pretnje iskoristi ranjivost	Učinak		
	Mali (10)	Srednji (50)	Veliki (100)
Velika (1,0)	10 x 1,0 = **10**	50 x 1,0 = **50**	
Srednja (0,5)	10 x 0,5 = **5**	50 x 0,5 = **25**	100 x 0,5 = 50
Mala (0,1)	10 x 0,1 = **1**	50 x 0,1 = **5**	100 x 0,1 = **10**

Prilikom procene rizika kompanije treba da utvrde nivoe rizika kome je izložen informacioni sistem i predloži mere zaštite u cilju smanjenja rizika na prihvatljivi nivo. Oni se procenjuju sa aspekta mogućih posledica uzrokovanih narušavanjem funkcionalnosti i/ili bezbednosti informacionog sistema. Potrebno je izvršiti analizu pretnji informacionom sistemu zajedno sa ranjivostima, kao i kontrolama koje su primenjene u informacionom sistemu. [483]

Tabela 25. *Primer lestvice rizika i aktivnosti koje je potrebno preduzeti*
Izvor:.[463]

Nivo rizika	Opis rizika i aktivnosti koje je potrebno preduzeti
Veliki rizik (veći od 51)	Ako je rizik procenjen kao veliki, nužno je hitno sprovođenje mera za smanjenje rizika. Postojeći sistem može da nastavi sa radom, ali potrebno je u što kraćem roku sastaviti plan sprovođenja mera i odrediti prioritete i rokove.
Srednji rizik (11 do 50)	Ako je rizik procenjen kao srednji, nužno je sprovođenje mera za smanjenje rizika. Potrebno je sastaviti plan sprovođenja mera kako bi se one sprovele u razumnom vremenu.
Mali rizik (1 do 10)	Ako je rizik procenjen kao mali, potrebno je utvrditi da li je neophodno sprovođenje mere za smanjenje rizika ili se rizik može prihvatiti.

Procena rizika trebalo bi da uključuje: [484]

- određivanje karakteristika sistema,
- identifikaciju pretnji,
- identifikaciju ranjivosti,
- analizu sistema kontrola,
- određivanje verovatnoće,
- analizu učinka,
- procenu rizika,
- predlaganje mera i
- dokumentaciju rezultata u obliku formalnog izveštaja.

Pouzdano određivanje bezbednosnih rizika je nemoguće bez adekvatne procene ranjivosti. Logika sistema upućuje na to da tamo gde nema rizika nema ni smisla ulagati u zaštitna sredstva. Vrši se implementacija samo onih zaštitnih sredstava koja će biti opravdana i adekvatna u pogledu zaštite poslovnih ciljeva kompanije. [485]

7.1.4 Ograničenja pri izboru mera zaštite

Implementacija mera zaštite ne garantuje uklanjanje rizika i pretnji, što može ukazati na postojanje preostalih (rezidualnih) rizika. Strukture upravljanja u kompanijama treba da budu svesne preostalih rizika sa aspekta njihovog mogućeg učinka i verovatnoće pojave negativnog događaja. U skladu sa tim donosi se odluka o prihvatanju preostalih rizika kojima je izložen informacioni sistem.

Pri izboru i implementaciji mera potrebno je razmotriti i ograničenja:

- organizacione prirode,
- finansijske prirode,
- određenog okruženja,
- vezana za ljudske resurse,
- vremenska ograničenja,
- pravna ograničenja,
- tehnička ograničenja,

- kulturološka i društvena ograničenja. [485]

Većinu njih najčešće definišu upravljačke strukture kompanije, tako da na njih utiče okruženje u kome kompanija posluje. Isto tako, potrebno je periodično revidirati ograničenja kako bi se identifikovala nova i uočile promene već poznatih ograničenja.

7.2 Sofistikacija malvera

Zlonamerni softver – malver (engl. *malware – malicious software*) predstavlja skup instrukcija koji namerno narušava bezbednosnu politiku informacionog sistema. Postoje razne vrste malicioznog softvera sa različitim načinima delovanja. Karakteristike malicioznog softvera prvenstveno odnose se na način njegovog širenja, dok su posledice delovanja skoro iste.[486]

Razmatrajući maliciozni softver potrebno je napomenuti da se nikad ne može u potpunosti verovati sistemu čije sve komponente nije napravio onaj ko ga koristi. Iako izvorni kod programa može biti prekontrolisan u potpunosti, ipak se u njega po izboru svog autora tokom kompilacije programa može ubaciti u kompajler maliciozni kod. Tako da ni pregled izvornog koda kompajlera ne može garantovati bezbednost programa.[487]

Tabela 26. *Tipični primeri zlonamernog softvera sa osnovnim karakteristikama*
Izvor: [489]

Tipovi	Karakteristike	Primeri
Virus	Inficira *host* fajl, samostalno se kopira, u većini slučajeva potreban mu je ljudski faktor da bi se samostalno kopirao (otvaranje fajla, čitanje mejla, butovanje sistema, ili izvrdavanje inficiranog programa).	*Michelangelo, CIH*
Crv	Širi se putem mreže, samostalno se kopira, u većini slučajeva nije mu potrebna ljudska interakcija da bi se širio.	*Morris Worm, Code Red, SQL Slammer*
Trojanski konj	Izgleda kao koristan program, ima prikrivenu malicioznu svrhu.	*Setiri, Hydan*
Adware, Spyware	*Spyware* – špijunski softver, *Adware* – reklamni špijunski softver, često se sadrže u drugim softverima.	*Gator, save*
Maliciozni mobilni kod	Čine ga mali programi skinuti sa nekog udaljenog sistema i pokrenuti lokalno sa minimalnim, ili bez učešća korisnika. Tipično pisani u: *Javascript, VB Script, Java* ili *ActiveX.*	*Sross Site Scripting*
Backdoor	Zaobilazi bezbednost sistema da bi omogućio pristup napadaču.	*Netcat, VNC*
Rootkit	Manipuliše sa srcem operativnog sistema, kernelom, sakriva i stvara backdoorove.	*Adore, kernel Intrusion System*
Kombinovan *malware*	Kombinacija više različitih tehnika prethodno prikazanih da bi stvorio bolji *malware.*	*Lion, Bugbear.B*

Maliciozni softver, obično čine dve komponente. Jedna komponenta omogućava umnožavanje i širenje malicioznog softvera na druge softvere i/ili računare. Drugu komponentu softvera čini izvršni maliciozni kod (engl. *payload*). Ovaj kod je upravo ono što autor malicioznog softvera želi da ostvari i zavisno od mašte autora i ograničenja

sistema može da radi različite stvari. [488]

U mnogobrojne probleme koji mogu da proizvedu zlonamerni softveri spadaju:

- uklanjanje osetljivih datoteka sa hard diska,
- dalje širenje zlonamernih akcija preko zaraženog računara,
- krađa podataka (lične i finansijske prirode),
- praćenje aktivnosti na računaru,
- prikupljanje podataka o navikama korisnika,
- skrivanje datoteka, procesa i mreže,
- upotreba zaraženog računara za skladištenje dodatnih zlonamernih kodova, ukradenih informacija, piratskog softvera i sl.

Širenje kroz sistem bez znanja i saglasnosti korisnika jedna je od glavnih osobina malicioznog softvera. Prema načinu na koji se širi u sistemu možemo ih podeliti na tri grupe: trojanski konji, virusi i crvi. [490] Još jedan način klasifikacije malicioznog softvera je i prema ponašanju na sistemu domaćinu, po nameni – svrsi za koju su napisani, ili prema efektima koje proizvode na samom sistemu. [491]

Savremeni maliciozni softveri danas vrše kombinovanje više vrsta malicioznosti i pokušavaju da iskoriste što više potencijalnih ranjivosti sistema. Danas je moguće kupiti kompletne alate (engl. *exploit kit*) koji tokom svoje aktivnosti na računaru žrtve izvršavaju sve aktuelne izvršne funkcije i svu kontrolu objedine u jednom panelu.

7.2.1 Trojanski konji

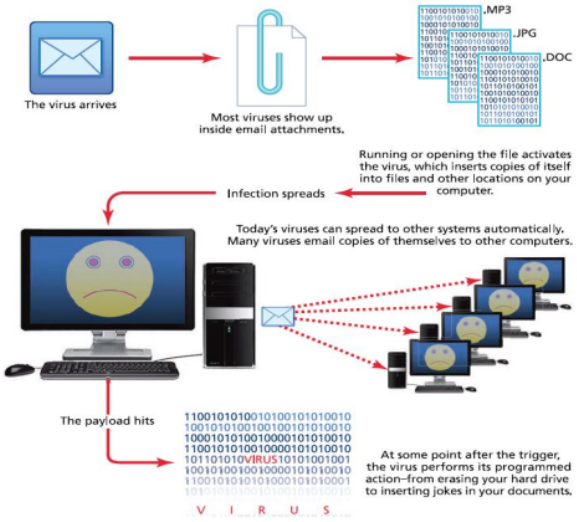
Trojanski konj predstavlja maliciozni računarski program. Termin Trojanski konj za maliciozni softver uveo je Dan Edwards, a njegova definicija je vremenom prilagođavana. [492] Termin se uglavnom odnosi na programe koji se predstavljaju kao da imaju neku korisnu namenu, ali u stvari imaju sakrivenu namenu koja koristi prava onoga ko ih pokrene. Razlog zbog čega je ovaj softver maliciozan leži u skrivenoj nameni koja može biti u suprotnosti bezbednosnoj politici informacionog sistema i koju nije lako otkriti. Može se ubaciti u računarski softver u vidu igrica, čuvara ekrana ili neki drugi program. Kada se jednom aktivira trojanski konj će napraviti štetu koja je predviđena dizajnom. Dizajniran je tako da se intervencijom čoveka prebacuje sa sistema na sistem. Kada neiskusni korisnici preuzmu i pokrenu takvu vrstu programa, on može izazvati brisanje datoteka, promenu podataka i prouzrokovanje nekih drugih vidova štete.

Danas postoji veliki broj programa koji pripadaju ovoj vrsti malicioznih softvera. S obzirom, da autor bilo kog malicioznog koda mora na neki način da sakrije njegovu malicioznost kako bi ga normalni korisnik izvršio postoje ramišljanja da se upravo svaki maliciozni program može nazvati trojanskim konjem. [491]

7.2.2 Virusi

U svojoj doktorskoj disertaciji Fred Cohen je 1986. godine pokazao kako se kod može prebacivati sa jednog računara na drugi i definisao pojam virusa kao *programa koji može zaraziti druge programe menjajući ih tako da uključe, moguće izmenjenu, verziju programa – virusa*. [493] Dokazao je i da je nemoguće napraviti program koji će potpuno tačno proveravati postojanje virusa. Sam Coen nije bio prvi koji je pomenuo niti pravio viruse. Von Neuman je 1949. godine u radu *Theory and Organization of Complicated Automata* [494] dokumentovao mogućnost pravljenja programa koji se umnožavaju, dok je

prvi samoumnožavajući program napravio John Conway 1970. godine. Nakon ovoga počeli su se pojavljivati i prvi maliciozni računarski virusi. Sagledavajući mnogobrojne definicije možemo zaključiti da je definicija Cohena najkompletnija i da virus predstavlja program ili kod koji je kreiran sa definisanim ciljem sopstvenog razmnožavanja u drugim datotekama sa kojima dolazi u kontakt. [495]



Slika 51. *Funkcionisanje virusa*
Izvor: [496]

Cilj virusa je širenje sa programa na program, ili sa diska na disk, koristeći pritom zaraženi program, datoteku ili disk za pravljenje što više svojih kopija. Obično se sastoji od dva dela. Prvi je samokopirajući kod, kojim se omogućava razmnožavanje virusa, dok drugi predstavlja korisni teret (engl. *payload*) koji može biti bezopasan (engl. *benigni*) ili destruktivan (engl. *maligni*).

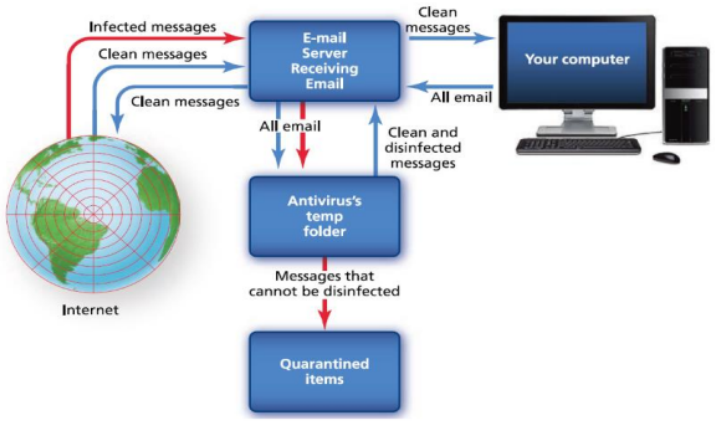
Najčešće se skriva u operativnom sistemu računara ili u aplikativnim programima i napravljen je za određen operativni sistem. Postoje i određeni izuzeci. Makro virusi povezuju sebe sa dokumentima koja koriste makroe i mogu da se šire preko različitih računarskih platformi. Mogu se širiti i preko e-mail priloga bezazlenog sadržaja pa se ponekad nazivaju e-mail virusi.

U odnosu na različite karakteristike viruse je moguće podeliti na mnogo različitih načina. Jedan virus može imati karakteristike više vrsta. Osnovni tipovi virusa su: [497]

- virusi koji vrše zarazu izvršnih datoteka,
- virusi koji se smeštaju u *boot* sektor diska i izvršavaju se kad god se računar pokreće sa tog diska ili prilikom prvog pristupa disku,
- svestrani virisi (engl. *multipartite*) koji vrše zarazu i *boot* sektora diska i izvršne datoteke,
- virusi koji ostaju aktivni u memoriji računara i nakon što program koji su zarazili računar prestane da se izvršava,
- prikriveni (engl. *stealth*),
- šifrovani virusi,

- poliforni virusi i
- makro virusi.

Prema stepenu opasnosti viruse je moguće podeliti na viruse koji uništavaju sistemske datoteke i imaju destruktivan uticaj na rad računara, pa sve do onih koji prenose šaljive poruke. Prema načinu prenosa razlikujemo viruse koji se šire putem makroa iz *Word* i *Excel* i putem prenosivih memorija. Najzastupljeniji način prenosa virusa je danas putem Interneta i prenos virusa putem Web sajtova i e-maila. Treće podela je prema vremenskoj zavisnosti – virusi koji se aktiviraju tačno određenog datuma. Bez obzira na grupu, svaki zlonamerni kod mora biti pokrenut da bi se izvršavao i razmnožavao. Razlikuju se u načinu na koji to pokušavaju da obezbede.



Slika 52. *Prikaz zaustavljanja virusa*
Izvor: [496]

Osnovne indikacije da u računaru postoje zlonamerni kodovi su: usporen rad računara, restartovanje računara bez zadavanja takve komande, samoinicijativno konektovanje na Internet, nepravilan rad pojedinih programa, brisanje sistemskih datoteka, nemogućnost pokretanja računara i dr. Najbolja zaštita je korišćenje antivirus softvera, kao i svakodnevno obnavljanje (engl. *update*) antivirusne baze uz redovno skeniranje računara. Poznavanje pravilnog rada na računaru i logičko razmišljanje korisnika u mnogome može doprineti smanjenju opasnosti koje vrebaju od strane virusa. Ono što je podjednako bitno je praćenje novih trendova napada i zaštite.

7.2.3 Kompjuterski crvi

Korisnici se uglavnom sreću sa kompjuterskim crvima (engl. *worms*), jer su klasični virusi retki. Kompjuterski crv predstvalja potklasu virusa. Obično se širi bez znanja i intervencije korisnika i sam distribuira sopstvene potpune kopije širom mreža. Predstavljaju tip malicioznog softvera koji se umnožava formiranjem novog procesaili datoteke sa svojim kodom. Ponašanje crva je takvo da može zauzeti memoriju ili propusni opseg mreže toliko da računar prestane da reaguje. Kada su u pitanju crvi nije obavezno da se i ostali programi inficiraju kao što je to slučaj sa virusima. Obzirom da im nije potreban softver-domaćin ili datoteka za prenos, mogu neprimetno da se uvuku u računarski sistem i omoguće daljinsku kontrolu inficiranog računar. [497]

Crvi u velikoj meri remete funkcionisanje mreže, štete podacima i kompromituju bezbednost računara. Dizajnirani su tako da mogu otrkriti druge računare sa specifičnim

osobinama u okruženju koji mu pružaju mogućnost uspešnog napada na sledeći računar i samostalne instalacije na njega. Ciklus se ponavlja dokle god ima novih računara koji su pogodni za širenje. Kompjuterski crv može da se umnožava sve dok se računar ne blokira usled nedostatka slobodne memorije ili prostora na disku. Tipičan segment kompjuterskog crva nalazi se u memoriji pre nego na disku, tako da se crv može eliminisati potpunim isključivanjem svih radnih stanica na mreži.

7.2.4 Adware

Podrška reklamiranju (engl. *adware*) predstavlja vrstu zlonamernog softvera koji automatski proizvodi reklamne poruke bilo da je to poruka u vidu *pop-up* prozora u pregledaču ili poruke koje se vide nakon pokretanja nekog drugog softvera. Često se dešava da se razni besplatni programi nude u paketu sa *adware* softverom koji omogućava jedan od modela za zaradu na besplatnom softveru. Ovakav softver najčešće nije opasan, ali može da iritira korisnike jer vrlo retko prikazuje relevantan sadržaj odnosno reklame koje bi bile relevantne za korisnika. Kako bi korisnik programa mogao da koristi verziju bez ovakvih reklama mora da plati neku obično veoma skromnu sumu novca.[497]

S druge strane, retko se dešava da *adware* ne ide u paketu sa *spyware* (špijunskim) softverom. On ima drugačiju namenu i predstavlja problem, jer neovlašćeno dostavlja informacije kako o sistemu, tako i o samom korisniku nakon čega se u kombinaciji sa *adware* može mnogo bolje targetirati korisnik da klikne na reklamu. One postaju sve relevantnije, a uzrok je pravljenje profila korisnika na osnovu ukradenih informacija.

7.2.5 Spyware

Šijunski softver (engl. s*pyware*) je vrsta softvera, koja u funkciji *adware* predstavlja njegovu prirodnu nadogradnju. Međutim, *spyware* se ne koristi samo u kombinaciji sa *adware* kako bi dostavio releventne reklame, već se češće korsti kao metod za ispitivanje ponašanja korisnika kroz krađu informacija. To čini najčešće podmetanjem super kolačića, sakupljanjem informacija o posećenim *web* lokacijama i generalno akcijama korisnika bilo na sistemu, bilo na Internetu. Na osnovu ovakvih informacija izrađuju se profili korisnika nakon čega autori *spyware* ovakve informacije prodaju trećim licima. Ta lica su obično marketinške agencije zainteresovane za analize tržišta ili druge agencije koje se bave ovakvim uslugama.[497]

Druga mnogo opasnija namena ovog softvera predstavlja prodaja ili zloupotreba informacija koje se tiču podataka o kreditnim karticama, socijalni brojevi kao i pristupne informacije za *e-banking* servise, društvene naloge i slično. Zlonamerni korisnik ovakve informacije može da iskoristi i na druge načine. Često se koristi ucena za povratak prikupljenih informacija. O tome će više reči biti u tački rada koji objašnjava *ransomware*.

7.2.6 Bot

Botovi predstavljaju vrstu softvera koji je napravljen da automatski realizuje određene operacije. Velika primena je u *on-line* igranju, takmičenjima, aukcijama i dr. Sve su popularniji i sve više se koriste u zlonamerne svrhe. Takvi botovi najčešće učestvuju u masovnim *DoS* napadima (engl. *Denial of Service, DoS*). Ovi, a i ostali, obično rade tako što se sa zaraženog računara kače na postojeći *irc* (engl. *internet relay chat*) kanal i tamo čekaju komandu autora. Botovi u zlonamernom smislu koriste se i kao paukovi koji redom skeniraju IP adrese i ukoliko naiđu na *echo* pokušavaju da zaraze servere i druge računare zlonamernim softverom.

Postoji primena i u vidu takozvanih sakupljača (engl. *harvestera*) raznih informacija od interesa za autora. Interes mogu biti e-mail adrese koje se posle koriste za

spamovanje korisnika ili širenje drugih zlonamernih napada. Iz ovog razloga često se vidi da programeri ili korisnici svesniji bezbednosti na svojim stranicama ne ostavljaju svoju e-mail adresu u ispravnoj formi već pišu nešto ovog tipa: dragansavic.rm[at]gmail.com. U harvester nije teško integrisati bilo kakvu varijaciju zapisa e-mail adrese da bi se prepoznalo nešto ovakvog tipa ili pak složenije. Međutim, kreatori takvog softvera to obično ne rade jer ukoliko je neko svestan toga da ne ostavlja svoju e-mail adresu po netu u korektnom obliku, onda je svestan i da ne bude žrtva *on-line* prevare ili greškom da otvori mail sa zlonamernim kodom.Odbrana od ovakvih vrsta virusa u smislu spam na netu su *captcha* testovi, koje može samo čovek da reši.

7.2.7 Bug

U kontekstu softvera *bug* predstavlja bilo kakvo neočekivano ponašanje softvera. Razmatrajući kontekst bezbednosti od manjih grešaka do onih većih najznačajniji su upravo bezbednosni bagovi. Ovakve greške se najčešće ne prave namerno već prosto kao posledica nemogućnosti da se pri razvoju sagleda svaki aspekt funkcionisanja softvera. Ali i pored ove činjenice postoje programeri koji iz ličnih motiva u softver na kome rade ostavljaju *backdoor* kako bi kasnije mogli da ucenjuju vlasnika softvera, imaju kontrolu ili postanu heroji kada otklone taj isti *bug*.

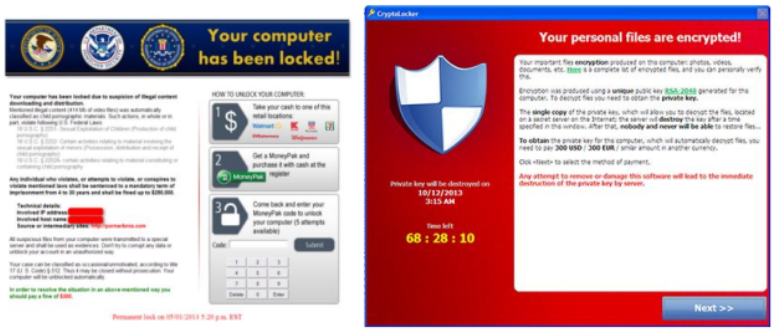
Mnogo bitniji kontekst jeste da bezbednosni bagovi ostavljaju prozor za ubacivanje malicioznog koda takozvanog *shell code*. Hakeri i drugi, svakodnevno traže ovakve bagove i pišu izvršne datoteke (engl. *exploit*) koji u stvari iskorišćavaju ove propuste. Ovakvi propusti u kodu se mogu predupredi dodatnom edukacijom programera na polju bezbednosti, pisanjem kvalitetnog i dobro testiranog koda, kao i korišćenjem neke od popularnih metodologija koje spuštaju prag napravljenih grešaka u istom.

7.2.8 Ransomware

Ransomver predstavlja tip malvera koja putem ograničavanja ili onemogućavanja korisnika da pristupi podacima na svom računaru iznuđuje novac (traži otkup). [498] U različitim oblicima postoji već decenijama, ali u poslednje tri godine, sajber kriminalci su ključne komponente napada doveli do savršenstva. Ovo je dovelo do eksplozije novih vrsta malvera koje su učinile tehnike napada efikasnijim i privukle nove maliciozne kreatore koji smišljaju i lansiraju ove unosne prevare. [499]

Da bi ransomware napad bio uspešan, napadači moraju da izvrše sledećih pet koraka:

- kompromitovanje sistema i uspostavljanje kontrole nad njim,
- onemogućavanje pristupa sistemu,
- upozorenje korisnika uređaja da im je sistem kompromitovan, obaveštavanje o ceni „otkupnine” i predlaganje koraka koje bi trebalo preduzeti,
- prijem novca od otkupnine i
- omogućavanje nakon isplate žrtvi potpun pristup sistemu.



Slika 53. *Poruka nakon što je Ransomware zarazio računar ili mrežu korisnika*
Izvor: [499]

Ranije verzije ransomvera koristile su zaključavanje sistem dok se kod današnjih verzija primenjuje tehnika šifrovanja datoteka. Korisnik dobija obaveštenje o radnjama koje su se odvile u njegovom sistemu u oba načina. Posle šifrovanja datoteka on se najčešće briše ostavljajući za sobom poruku o otkupu. Da bi dešifrovali blokirane datoteke korisnici moraju platiti otkup podataka u okviru nekog vremenskog perioda. U tom slučaju, napadač često preti da će izbrisati sve datoteke pri isteku vremena ili će uvećati iznos otkupa. [500]

Ransomver najčešće dospeva u sistem putem zaraženih web sajtova, kao deo nekog drugog malvera ili preko tzv. *phishing* kampanja. Kreatori su im veoma inovativni i neprekidno smišljaju nove taktike napada. [499] Od 2005. godine, ransomware malver se razvija u dva pravca – kao *scareware* i kao kriptografski *ransomware*. Sredinom 2005. godine pojavljuje se nova vrsta *crypto ransomware* – *GPCode* ili *PGPCoder*. Poslednji veliki talas *scareware* dogodio se 2011. i 2012. godine kada se pojavio *locker ransomware*. Najpoznatiji bio je *Reveton*. Nakon ovoga, maliciozni hakeri smišljaju kako bi mogli da povećaju efikasnost iznuda. Odgovor se javlja 201 godine u vidu *CryptoLocker*-a koji šifruje fajlove na operativnom sistemu *Windows*. Neki od njih su: *Crypt0L0cker* virus, *CryptoLocker-v3*, *Cryptografic Locker*, *PCLock ransomware* *CryptoTorLocker 2015*, *CryptoWall*. Početkom 2014. godine pojavio se novi ransomver *Crypto Wall*. U svom radu koristi *AES*šifrovanje, *CHM* mehanizam za propagaciju i *Tor* anonimnu mrežu. Postoji više varijanti *Crypt Wall* i to: *Cryptorbit*, *CryptoDefense*, *CryptoWall 2.0, 3.0* i *4.0*. [501][502] U martu 2016. godine, otkriven je malver *KeRanger*, koji predstavlja prvi dokumentovani ransomware napad na *Mac OS X* sisteme.

Široko rasprostranjeni su i sledeći ransomver-i:

- *TeslaCrypt* koji je orijentisan na korisnike *on-line* igrica,
- *SamSa* koji prvenstveno napada sektor zdravstva,
- *Locky* koji je fokusiran uglavnom na region Nemačke i Holandije,
- *Petya* ransomver koji napada *boot* sektor sistema,
- *KeRanger* koji je dizajniran za iOS sisteme kao i
- ransomver koji napadaju Android sisteme.

S obzirom na činjenicu da se ransomware pokazao izuzetno isplativim kriminalnim poslom, u budućnosti možemo očekivati:

- više platformi – nijedan operativni sistem više nije imun na napade i svaki uređaj može biti meta napada,

- viši iznosi otkupnina i
- ciljane ransomver napade.

Kako bi se odbranili potrebno je biti svestan pretnje i napraviti plan za njeno sprečavanje. Odbrana se može raščlaniti na tri dela: pripremu, prevenciju i odgovor (reakciju). U procesu pripreme odbrane od ransomvera razlikujemo: *Backup* i *Recovery* proces, kao i kontrolu pristupa zajedničkom prostoru na mreži.[503] Najveći broj napada ransomver događa se dok korisnici surfuju Internetom ili dok čitaju e-mail, zato se na ovo mora obratiti posebna pažnja. Ključ u prevenciji odbrane je u sprečavanju malvera da uopšte uđe u sistem i šifruje važne podatke. Ukoliko prevencija nije uspela i ako ste postali žrtva ransomware napada, važno je da imate pripremljen plan kao odgovor na napad. On će vam pomoći da u što kraćem roku i uz najmanje štete po kompaniju vratite svoje podatke.[504]

Dobru praksu u zaštiti od napada je korišćenje anti-virus programa i *firewall*-ova koja često nije dovoljna. Jedan od pristupa za prevenciju ransomvera je filtriranje sadržaja. Web guard sistem predstavlja efektivnu zaštitu jer vrši potpunu dekompoziciju i odbacivanje svega osim poslovnih informacija. [505] Neka od rešenja za zaštitu na aplikativnom nivou su *Mail guard* za zaštitu e-mail saobraćaja, *File Transfer guard* za bezbedan prenos datoteka, *XML guard* za kontrolu XML saobraćaja, *TransGap Import Export* za kontrolu datoteka koje se uvoze/izvoze na medijume itd. Kod složenih sistema najbolja zaštita od ransomvera, ali i drugih sajber napada je kombinovano korišćenje više rešenja iz domena zaštite na aplikativnom nivou. Kombinacijom predstavljenih rešenja i pravilnom edukacijom zaposlenih sistem se može zaštititi od bilo kog sajber napada ili kombinacije napada.

7.2.9 Rootkit

Rootkit predstavlja mali deo softvera dizajniranog da kontroliše računar na daljinu bez mogućnosti da bude otkriven od strane korisnika ili antivirusnog softvera. Ima mogućnost da na daljinu izvršava druge programe, menja konfiguraciju sistema pa i sam sistem. Zbog ovakvih mogućnosti veoma je teško otkrivanje od strane antivirusa jer preuzima potpunu kontrolu nad procesima i sveukupnim kontrolisanjem sistema.[506]

Eventualno otkrivanje rootkit svodi se na praćenje neregularne aktivnosti sistema, statističku proveru korišćenja određenih servisa operativnog sistema, ili proveravanje potpisa. Zaštita je kao i za sve ostale ozbiljne pretnje preventivne prirode u smislu instaliranja zakrpa ranjivog softvera, i pažljivo podešavanje zaštitnog zida *(firewall)*.

7.3 Napadi

7.3.1 Napadi nultog dana

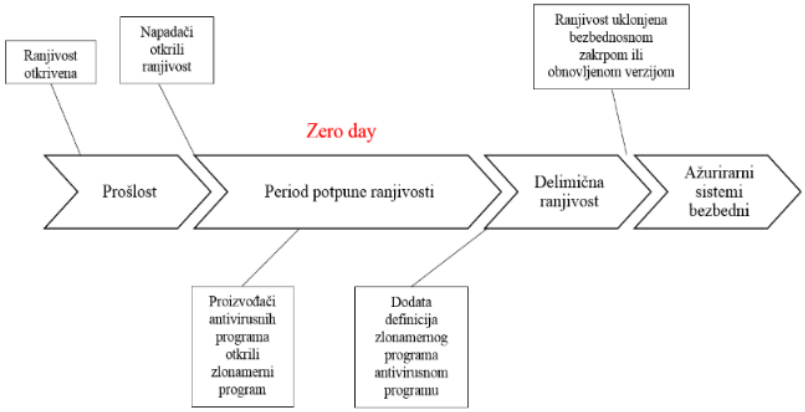
Napadi nultog dana (engl. *Zero day attack*) predstavljaju bezbednosni propust u računarskom softveru koji su otkriveni i poznati hakerima pre nego što za njih znaju proizvođač i javnost. Takva ranjivost nema zakrpe od strane proizvođača. Izraz „nulti dan" nastao je kao vremenska oznaka ranjivosti. Ovaj napad se obično javlja pre nego što proizvođač postane svestan o ranjivosti u softveru, što znači da on nije imao priliku da ispravi bezbednosni propust koga napadač koristi za napade. Vreme detekcije ranjivosti obično traje od nekoliko dana do nekoliko nedelja. Napadači koji izvedu uspešan napad iskorišćavanjem ranjivosti nultog dana se u hakerskom svetu smatraju se elitom, jer je otkrivanje takve ranjivosti i izvođenja napada teško. U tu svrhu je neophodan visok nivo

poznavanja programskih jezika, struktura programa u kome se traži ranjivost, mreža računara, operativnih sistema, kao i iskustvo, snalažljivost, trud ali i inovativnost.

Otkrivanje i uklanjanje ranjivosti nultog dana izvodi se kroz nekoliko faza u kojima opasnost od eksploatacije ranjivosti raste i opada sa vremenom. [507]

Vremenski period u kom postoji bezbednosna pretnja koja još uvek nije objavljena i/ili priznata naziva se *less-than-zero* ranjivost. Ranjivost nultog dana predstavlja veliki rizik za korisnike, dok *less-than-zero* ranjivost ne nosi sa sobom veliki rizik. Većina njih se otkriva raznim testovima ranjivosti tako da ona postane poznata pre nego što je poznat način njene zloupotrebe. Otkrivanje *less-than-zero* ranjivosti se javlja nakon što se uoče dokazi o zlonamernom programskom kodu. Životni ciklus ranjivosti predstavlja sledeće:

- postojanje ranjivosti,
- ranjivost otkrivaju zlonamerni korisnici,
- otkriveni zlonamerni programi koji iskorištavaju ranjivost,
- detekcija zlonamernog programa dodata u bezbednosne programe za detekciju,
- razdoblje delimične ranjivosti i
- ranjivost je uklonjena objavom zakrpe ili obnovljene verzije.



Slika 54. *Životni ciklus ranjivosti*
Izvor: [507]

Ova vrsta napada predstavlja specifičnu vrstu bezbednosnih propusta te običnom korisniku bude teško da se zaštiti od njih. Ako se računari i softveri koriste na pravilan način, postiže se jedan prirodni nivo zaštite u tom okruženju. Ažurne baze antivirusnih softvera i drugih alata koji otkrivaju zlonamerni programski kod neće pružiti zaštitu od napada. Preporučuje se pravilna implementacija *firewall*-a koji može sprečiti pokretanje zlonamernog programskog koda. Treba izbegavati programske pakete za koje je poznato da nisu bezbedni jer se u njima često javljaju bezbednosni propusti. Objavljene bezbednosne zakrpe od strane proizvođača softvera potrebno je primeniti što je pre moguće kako bi korisnik zaštitio svoj računar. Da bi iskoristili i naveli korisnika da im pomogne u izvođenju napada bez znanja da to čine, napadači se često služe socijalnim inženjeringom.

7.3.2 Ciljani napadi

Napadači koriste svu raspoloživu tehnologiju kako bi razvili svoje načine napada. Sve ovo dovodi do velike promene u samim profilima napada. Ono što se danas može videti je postojanje elitnih hakerskih grupa, koje su dobro organizovane, pripremljene i opremljene sa ekstremno velikim brojem kvalitetnih softvera (napadačkih alata) za napada na tuđe sisteme. [508] U poređenju sa komercijalnim softverima hakerski softver (napadački alat) je veoma dobro urađen i oslobođen od grešaka. Lak je za korišćenje i dizajniran tako da podržava široku skalu napada, uvećavajući moć potencijalnih napadača. U suprotnosti tome, na drugoj strani nalaze se oni koji se bave zaštitom i koji nisu privrženi principu deljenja informacija. [509]

Od posebnog značaja je podatak da izvorni kod više nije neophodan kako bi se otkrile slabosti ciljanog sistema, što povećava broj onih koji su u stanju da izvrše napad. Ako se pri tome doda podatak da su napadi preko Interneta relativno laki, niskog rizika i teški za praćenje, onda je jasno koju težinu u celom kompleksu imaju ciljani napadi. Povoljnim mogućnostima napada na sisteme značajno doprinsi i rapidna adaptacija informacione tehnologije u vladinim, korporacijskim i akademskim organizacijama, ekspanzija Interneta i korišćenje mogućnosti elektronske trgovine, enorman broj prisutnih slabosti u tehnologiji koje se mogu iskoristiti, i relativno nizak nivo svesti o potrebi zaštite. [510]

Već ranije je navedeno da pretnja predstavlja mogućnost narušavanja bezbednosti. Akcije kojima se pretnje ostvaruju i od kojih se treba štititi nazivaju se napadi. Posedice pretnji se mogu podeliti u četiri kategorije: [511]

- otkrivanje (engl. *unauthorized disclosure*) – neovlašćeni pristup informacijama,
- prevara (engl. *deception*) – prihvatanje pogrešnih podataka,
- smetnja (engl. *disruption*) – prekidanje ili sprečavanje normalnog rada i
- uzurpacija (engl. *usurpation*) – neovlašćena kontrola nekog dela sistema.

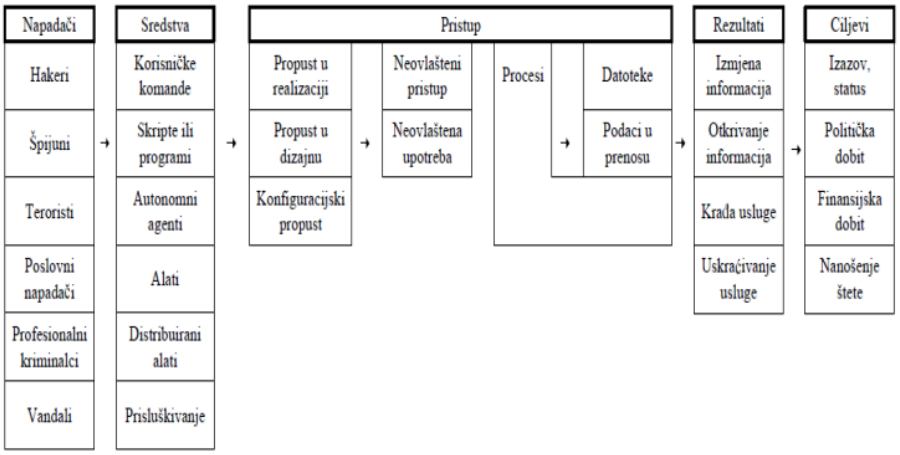
Napadi mogu proisteći iz pretnji. U suštini, to su akcije koje su usmerene na ugrožavanje bezbednosti podataka, računarskih sistema i mreža. Postoji brojna literatura koja se bavi problematikom sistematizacije napada. Najčešće korišćena podela napada prema Jones i ostalima je: [512]

- izviđanje – testiranje potencijalne mete radi prikupljanje informacija,
- onemogućavanje pružanja usluge (engl. *Denial of Service*,*DoS*),
- pristup sa daljine (engl. *Remote to Local*, *R2L*) i
- podizanje privilegija (engl. *User to Root*, *U2R*).

Sled događaja prilikom napada može se razdvojiti u tri faze, tvrdi Vacca: [513]

- vreme pre napada,
- izvođenje napada i
- iskorišćavanje uspešno izvedenog napada.

Napadači imaju ciljeve i ostvaruju ih koristeći sredstva koja im omogućavaju pristup čime ostvaruju svoj cilj.

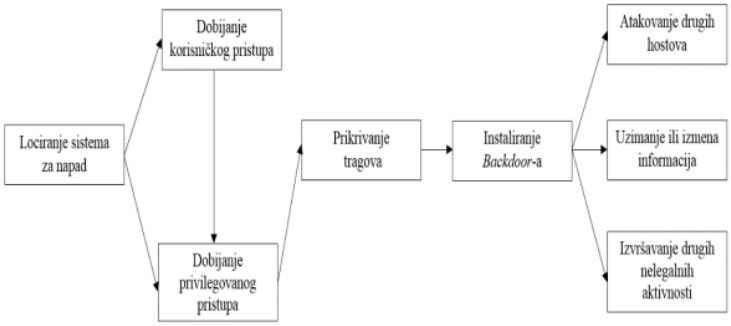


Slika 55. *CERT sistematizacija i način povezivanja svih faktora u sekvenci ugrožavanja bezbednosti*
Izvor: [514]

Generalno se napadi klasifikuju u četiri osnovne kategorije: [515]

- presecanje, tj. prekidanje (engl. *interruption*) predstavlja napad na dostupnost (engl. *availability*),
- presretanje (engl. *interception*) predstavlja napad na poverljivost (engl. *confidentiality*),
- izmena (engl. *modification*), predstavlja napad na integritet (engl. *integrity*),
- fabrikovanje (engl. *fabrication*), predstavlja napad na autentičnost (engl. *authenticity*).

Tipičan ciljani napad na udaljene sisteme, korišćenjem automatizovanih napadačkih alata, realizuje se u vremenu koje se meri sekundama. Pri tome, napadač je zainteresovan ne samo da dobije pristup do podataka na napadnutom - ciljanom računaru, već i da taj računar koristi kao lansirnu rampu za kompromitovanje drugih sistema, otežavajući tako trasiranje njegovih aktivnosti (slika 56).



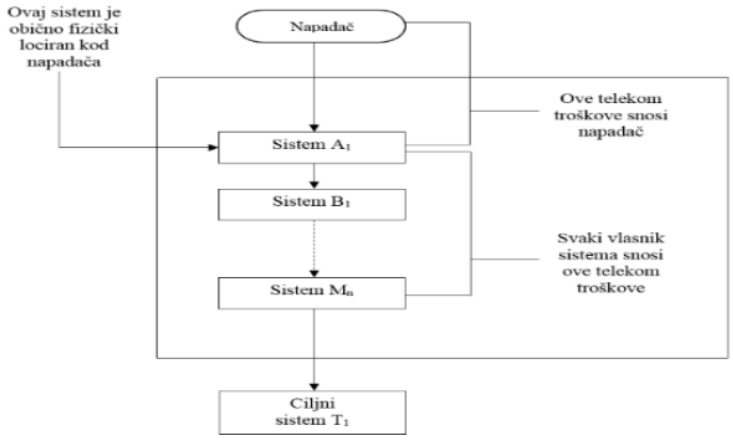
Slika 56. *Tipičan ciljani napad*
Izvor: [516]

Upravo zahvaljujući ovakvom pristupu nastao je jedan ozbiljan fenomen koji se često previđa, a to je razvijanje virtuelne, ilegalne računarske mreže. Ova mreža je

formirana od sistema u koje je napadač već prodro i kompromitovao ih.[517] Napadač, nakon upada u ciljani sistem, nastavlja proces upada i kompromitovanje drugih sistema. Sistemi mogu pripadati različitim vlasnicima, locirani bilo gde i biti povezani u različite mreže. Međutim, ovi ciljani sistemi su sada uključeni u jednu virtuelnu računarsku mrežu, raspoloživu za korišćenje od strane napadača.[516]

Nakon upada u ciljani sistem, napadač mora da brine o sledećem: kako da spreči otkrivanje aktivnosti; kako da redukuje ili eliminiše telekomunikacione troškove; na koji način da izvrši transfer i skladištenje informacija – podataka; kao i da sakrije performanse mreže.

Napadač prvo pristupa prethodno kompromitovanom sistemu. Ovaj sistem se onda koristi kao sistem koji omogućava konekciju sa narednim kompromitovanim sistemom itd. Na taj način napadač „skače" od jednog sistema do drugog kroz „svoju" virtuelnu mrežu. U većini slučajeva napadač će koristiti dva do tri sistema pre nego što napadne ciljni sistem. U ovom slučaju, ako se na ciljnom sistemu otkrije pokušaj upada, moći će se samo konstatovati da aktivnost dolazi sa sistema. Isto tako, sistem će samo videti aktivnosti sa sistema itd. Manje od tri sistema čine relativno lakim traganje unazad za ilegalnim aktivnostima, dok više od pet sistema počinje da degradira performanse „podzemne"– virtuelne mreže.



Slika 57. *Tradicionalni uzorak aktivnosti napadača*
Izvor: [516]

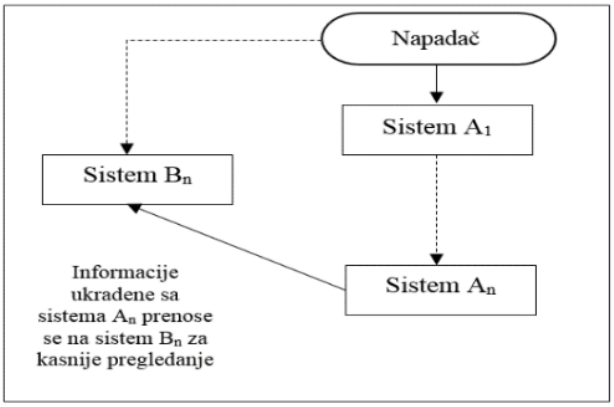
Na slici 57, takođe je prikazano kako napadač redukuje telekomunikacione troškove. U klasičnom slučaju, sistem je blizak napadaču tako da on sam snosi lokalne troškove. Međutim, svi ostali sistemi u lancu su geografski udaljeni što je moguće dalje i legitimni vlasnici snose telekomunikacione troškove konekcije sa narednim sistemom. To omogućava napadaču da napadne neki sistem bilo gde na svetu i da za konekciju plati samo lokalne troškove. Da bi još više iskomplikovao traganje i redukovao rizik da vlasnik nekog od sistema uoči visoke telekom troškove, napadač će održavati konekciju sa sistemom što je moguće kraće (obično od 5 do 15 minuta). Posle toga konekcija se prekida, a nova se uspostavlja po istoj metodologiji, ali sada sa potpuno drugim sistemima. Na ovaj način, na ciljnom sistemu će se moći uočiti da napadi dolaze iz različitih izvora širom sveta, mada, u stvari, postoji samo jedan jedini napadač. Najzad, da poveća konfuziju otkrivanja, napadač može plasirati informacije da pristupa napadnutom sistemu na nekom

BBS-u ili sličnom javnom forumu. To obično rezultira stotinama pokušaja pristupa od različitih napadača, čineći izuzetno teškim separaciju i identifikaciju aktivnosti originalnog napadača.

Kao što je već potencirano, ovo je tradicionalni uzorak (način) napada. Međutim, sa stanovišta napadača postoji nekoliko slabosti. Prvo, ako vlasnik sistema otkrije aktivnost, traganje neće biti teško. Drugo, održavanje dovoljnog broja sistema u „podzemnoj" – virtuelnoj mreži konzumira puno vremena. Napadač, takođe, mora kontinuirano napadati i kompromitovati sisteme da bi održavao ilegalnu mrežu, posebno ako sistem administratori eventualno otkriju ilegalnu aktivnost i zaštite sistem. Dakle, trenutni trend je napad na telekomunikacionu infrastrukturu kako bi se obezbedila što direktnija konekcija sa ciljnim sistemima uz manje troškove i redukovanje mogućnosti otkrivanja i traganja.

Drugi značajan i opšti uzorak je transfer i skladištenje informacija. Kada je napadač zainteresovan za informacije na sistemu, on će često želeti da dobije kopiju informacija za njihovo kasnije korišćenje ili detaljnije pretraživanje. Čak i sa povećanim raspoloživim memorijskim prostorom na svom računaru, napadač će često biti u situaciji da mu nedostaje prostor za smeštanje velikog obima ukradenih informacija. Dakle, on će koristiti tuđe sisteme za privremeno skladištenje ukradenih informacija. Prenos i skladištenje ukradenih informacija unutar „podzemne mreže" prikazani su na slici 58.

U ovom primeru, napadač nalazi informacije od interesa na sistemu. Ove informacije on kopira na sistem. U nekim slučajevima ove informacije mogu biti smeštene na većem broju sistema i sve to bez znanja legitimnih vlasnika. Kasnije, napadač može pristupiti ukradenim informacijama, pregledati ih ili ih preneti na drugu lokaciju. Takođe, ove informacije može staviti na raspolaganje drugom napadaču ili drugim zainteresovanim licima jednostavno dajući im lokaciju sistema (telefonski broj modema) na kojem su informacije smeštene i kako da pristupe sistemu (*User ID* i lozinku). Na ovaj način informacije mogu biti ukradene, prenete preko državnih granica i prodate, a da napadač nijednog trenutka fizički ne poseduje ova dokumenta, niti vlasnik može znati da je pokraden. Najzad, napadač mora izbalansirati sve ove aktivnosti sa mrežnim performansama. Kao što je rečeno, većina napadača održava vezu sa ciljnim sistemom veoma kratko vreme i za to im je potreban brz odgovor. Takođe, kada se prenosi veliki obim podataka, mrežne performanse su kritične. Dakle, zahteva se duže vreme konekcije, što omogućava potenciljano otkrivanje.



Slika 58. *Prenos i skladištenje ukradenih informacija*
Izvor: [516]

Prema podacima u istraživanju koje je vodio Don B. Parker i njegov tim u *SRI*

International u Menlo Parku, Kalifornija, SAD, pretnjama informacionim sistema pripisuju se brojne aktivnosti, među kojima posebnu pažnju zaslužuju: nezakonit ulazak u računare u domenu biznisa, bankarstva, vladinih agencija, telefonskih kompanija, istraživanja, medicinske zaštite, kredita, akademskih institucija; uništavanje velike količine poslovnih, istraživačkih, vladinih, privatnih i drugih informacija i sl. [518][519].

7.3.3 Interni napadi

Napadači iznutra u komapnijama mogu da kompromituju veliki deo podataka kompanija. Možemo razlikovati dve vrste insajdera. Prvu predstavljaju zaposleni koji koriste svoj privilegovan pristup i mogu svojim aktivnostima da oštete svoje poslodavce. Drugu predstavljaju infiltratori koji rade za neku drugu kompaniju ili žele da prodaju poverljive informacije na crnom tržištu. Zlonamerne insajdere koji imaju pun pristup informacionom sistemu određene kompanije veoma je teško zaustaviti, dok je politiku bezbednosti koja sprečava curenje podataka, veoma teško održavati.

Sve više kompanija beleži rizike koje insajderi mogu predstavljati bezbednosti podataka u kompaniji. Proboji u informacione sisteme i eventualna krađa podataka, obično se izvršava izvan kompanijskih informacionih sistema i ove pretnje uopšte rešavaju se tradicionalnim bezbednosnim merama u informacionim sistemima. Međutim, pretnje koje dolaze iznutra mnogo je teže sprečiti i otkriti pomoću bezbednosnih mera.

Insajderi zaposleni u kompaniji imaju pristup osetljivim informacijama kroz redovno izvršavanje svojih poslovnih funkcija u kompaniji i mogu znati kako su te informacije zaštićene. Ako žele da ukradu ili propuste podatke, obično to mogu učiniti jednostavno i lako u odnosu na lica koja nisu zaposlena i nalaze se van kompanije. Politika bezbednosti u kompaniji i tehnologije, mogu pomoći u rešavanju ovog rizika. Propuštanje podataka koje potiče iz grešaka pojaviće se kao rezultat delovanja unutrašnjeg entiteta kompanije.

Interni napad nastaje kada pojedinac ili grupa unutar kompanije nastoje da poremete operacije u kompaniji ili iskoriste njenu imovinu. U mnogim slučajevima napadač iskorišćava značajnu količinu resursa, alata i veština za pokretanje sofisticiranog računarskog napada i potencijalno uklanjanje dokaza o tom napadu. Visoko kvalifikovani i nezadovoljni zaposleni (kao što su administratori sistema i programeri) ili tehnički korisnici koji bi mogli imati koristi od ometanja operacija u kompaniji mogu preko svojih računarskih sistema izabrati pokretanje unutrašnjeg napada na kompaniju.

Jedan od najboljih načina zaštite od internih napada predstavlja implementacija sistema za otkrivanje upada i konfigurisanje skeniranja za spoljašnje i unutrašnje napade. Većinu bezbednosnih mera potrebno je logički povezati sa mrežnim perimetrom koji štiti interne mreže od spoljnih veza kao što je Internet. Dok je perimetar mreže zaštićen, unutrašnji ili poverljivi deo mreže teži da bude mekan. Kada napadač prvi put prođe kroz tvrdu spoljnu školjku mreže, kompromitovanje jednog sistema za drugim, obično je veoma jednostavno.

Možemo razlikovati sledeće rizike kompanija, koji se tiču upotrebe informacione tehnologije u kompaniji: [518][519]

- neovlašćeni pristup – korisnički/programerski pristup nije bio odobren za određeni nivo pristupa ili aktivnosti,
- prekomeran pristup – korisnički/programerski nivo pristupa prevazilazi njihov opis posla, i s njim u vezi odgovornosti,

- neovlašćene izmene – programska izmena nije odobrena pre nego što se krenulo u produkciju,
- prevara – potencijalan rezultat ovih rizika ukoliko su aktivnosti namerne,
- manjak kontrole vezan za nabavku i primenu novih aplikacija i održavanja postojećih aplikacija i
- manjak kontrole vezan za nabavku, instalaciju, konfiguraciju, integraciju i održavanje IT infrastrukture.

Korisni okviri kao osnova za okruženje interne kontrole informacionih sistema su:

- *COSO/COSO ERM*,
- *COBIT (ISACA)*
- *ITIL*,
- *CMMi* (*Capability Maturity Model*),
- ISO 20000,
- ISO 27001 i
- *RiskIT (ISACA)*.

Metode za preventivne i detektivne kontrole kod internih napada su:

- segregacija dužnosti – operativni i privilegovani pristup,
- dvofaktorska i višefaktorska autentifikacija,
- periodični pregled uloga i pristupa na svim nivoima, od pristupa mreži do pristupa aplikaciji (najmanje jednom u šest meseci),
- monitoring kontinuiranih kontrola – automatizovan i mauelni kroz praćenje pristupa sistemima, promena iz izvora (aplikacija/baza podataka/operativni sistem), i praćenje *firewall* aktivnosti,
- šifrovanje podataka u tranzitu i
- razmatranje *firewall* aplikacije.

Prilikom razmatranja događaja na višem nivou mnogi stručnjaci za informacionu bezbednost, pokušavaju da razmotre uloge uzimajući u obzir mehanizme unutrašnje kontrole kao što su: dvostruke kontrole i segregacije dužnosti. Obe ove kontrole primenjuju se za sprečavanje ili smanjenje prevara, ali se neznatno razlikuju u svojim ciljevima.

IT sistem predstavlja osnovu poslovanja svake moderne kompanije. Međutim, ova osnova može da postane problematična, ukoliko se ne razmatre rizici i pretnje. Neki rizici nisu očigledni, pa često zaboravljamo na njih, što je pogrešno, jer se skriveni rizici IT sistema često javljaju bez upozorenja i mogu stvoriti velike probleme. Izdvojili smo neke od najvećih skrivenih pretnji po IT bezbednost na koje treba obratiti pažnju, a to su:

- sistemi koji se ne koriste,
- nekontrolisan pristup,
- manuelni backup,

- „rupe" u mehanizmu bezbednosti,
- eksterne aplikacije,
- oprez sa korišćenjem *Byod* uređaja i
- slabe lozinke (ili ne korišćenje lozinki).

Kriminalni napadi mogu se dogoditi iznutra, od strane zaposlenih u napadnutoj kompaniji. Kada je u pitanju kršenje IT bezbednosti, manje i srednje kompanije su jedinstveno ranjive jer mogu da imaju nedostatak sofisticiranih sistema za otkrivanje i detekciju upada koje koriste velike kompanije. Razlog tog nedostatka je pre svega u nerazumevanju pretnji. Ima pet napada koji mogu da se dogode:

- maliciozni sajber napadi (engl. *malicious cyberattacks*),
- socijalni inženjering (engl. s*ocial engineering*),
- skidanje malicioznog sadržaja sa Interneta (engl. *downloading malicious internet content*),
- curenje informacija (engl. *information leakage*) i
- ilegalne aktivnosti (engl. *illegal activities*).

7.4 Zaštita kontejner tipa

Osnovne vrste zlonamernog softvera prave štetu računarima i podacima, remete konekciju s Internetom i upotrebljavaju računar kako bi se dalje širili. U nastavku rada biće reči o antivirusnoj zaštite, metodama saznanja da li je računar napadnut kao i rešenjima uz čiju pomoć se može podići nivo bezbednosti računara. [520]

7.4.1 Antivirusna zaštita

Opasnost od malicioznih softvera bio je razlog pojavljivanja čitavih grana IT industrije koja se bavi proizvodnjom alata za otkrivanje i uklanjanje ovih softvera. Dva najpoznatija i najčešć alata su antivirus i *antispyware*. [521]

7.4.1.1 Metode antivirusnih softvera

Prilikom otkrivanja malicioznih programa antivirusni softver koristi nekoliko metoda. Prva metoda rada antivirusnog softvera je skeniranje. [521] Ova metoda vrši 53dicionalno prepoznavanje virusa na temelju ugrađenih podataka u njemu. Ti podaci su pribavljeni analizom virusa koji se pojavio među korisnicima. Mogu da se odnose na niz heksadecimalnih znakova (engl. *search string*) – koji nekada mogu sadržati i *wildcard* (džoker) znakove.

Antivirusni softveri analiziraju datoteke, sektore na hard siku i sistemsku memoriju u potrazi za poznatim i nepoznatim malicioznim kodom. To je u stvari pretraga datoteka za poznatim nizom bajta karakterističnim za virus. Antivirusni softveri skladište sve definicije u neku bazu podataka na osnovu koje vrše pretraživanje. Kako se stalno pojavljuju novi virusi, kompanije koje proizvode antivirusni softver stalno proizvode i nove definicije. Ove definicije je potrebno distribuirati do antivirusnih programa. Obično, sami antivirusni programi pristupaju centralnoj bazi podataka proizvodača iz koje vrše ažuriranje svojih definicija. Očigledno je da je za prepoznavanje malicioznog koda potrebno imati njegov potpis, pa se novi virusi za koje antivirusni program još nema definiciju ne mogu ni prepoznati. Glavna prednost ove metode ogleda se u mogućnosti trenutne detekcije

poznatih virusa jednostavnim pregledom sumnjivog sadržaja. Ukoliko antivirusni softver prepozna virus, on će izvestiti korisnika o kom se virusu radi, što je važno, jer se prema tom podatku mogu proceniti i moguće posledice napada virusa. Nedostaci ove metode su u potrebi za stalnim dograđivanjem antivirusnog softvera radi prepoznavanja novih virusa, ali i nemogućnosti prepoznavanja virusa o kojima softver nema neophodne podatke. [521]

Druga metoda u otkrivanju malicioznog softvera je kada antivirusni softver pokušava da otkloni problem nepostojanja definicija. Ovaj pristup se naziva heuristički. Ideja ovakvih antivirusnih softvera je da nije neophodno imati tačan potpis za svaki virus, već je dovoljno prepoznati deo koda ili imati opšte definicije koje pokrivaju više virusa ili više varijanti polimorfnog virusa. Takođe, moguće je prepoznati virus i po delovanju, ali to može biti prekasno. Iz ovog razloga neki antivirusni softveri omogućavaju pokretanje sumnjive datoteke izolovanom okruženju (engl. *sandbox*) i tu otkrivaju maliciozno delovanje. [521]

Treća metoda u otkrivanju malicioznog softvera je provera integriteta bitnih, najčešće izvršnih, datoteka na sistemu računanjem *checksum*-e ovih datoteka. Tehnika provere *checksum* zasniva se na mogućnosti prepoznavanja svake promene na štićenom sadržaju. Njome se izvrši „zaleđivanje" stanja sistema za koji je potrebno utvrditi da li je zaražen. Nakon toga se u određenim vremenskim razmacima proverava da li je na sistemu došlo do nekih promena. Ideja je da za sve bitne datoteke postoji baza podataka sa vrednostima *checksum* za ispravne verzije ovih datoteka. Ove vrednosti iz baze se porede sa onim izračunatim nad tekućim datotekama u sistemu i ako postoji razlika otkriva se da su datoteke na sistemu izmenjene. *Checksum* je jedina poznata metoda kojom se sa sigurnošću otklanjaju virusi, bez obzira na to da li su poznati ili ne. Upravo joj činjenici leži dugoročni oslonac svake mudre antivirusne strategije. Nedostatak joj je da se njima otkriva infekcija virusom tek nakon što se ona već dogodila, međutim, njihovom redovnom primenom sigurno se može otkriti virus pre nego što dođe do značajne štete u računaru. [521]

Četvrta metoda rada antivirusnih softvera je monitoring. Ovom metodom prati se odvijanje pojedinih funkcija sistema preko odgovarajućih *interrupta*. Neki pokušavaju otkriti sumnjive aktivnosti pre potrage za specifičnim virusima. Jedina prednost monitora je da u realnom vremenu mogu otkriti virus. Najveći nedostatak monitora je nemogućnost delotvorne primene programa koji bi u sebi sadržao podatke za prepoznavanje svih poznatih virusa.

Još jedan od načina zaštite od malicioznog softvera je kontrola razmene datoteka, odnosno puteva kojim se zlonamerni softver širi. Potrebno je kontrolisati medije za prenos datoteka (USB flash memorije i dr.) pre nego što se sa njih pokrenu ili kopiraju datoteke. Ipak, da bi se smanjila opasnost od širenja zaraza ovim putem potrebno je obustaviti korišćenje medijuma za prenos podataka nepoznatog porekla. To je više stvar obuke korisnika nego tehničke implementacije. Slično se odnosi i na repozitorijume za razmenu datoteka. Ovi repozitorijumi mogu biti pod kontrolom kompanije, ali danas su oni sve češće na Internetu i u potpunosti van kontrole kompanije.

7.4.1.2 Organizacione mere antivirusne zaštite

Sve mere zaštite ne mogu biti dovoljne ako korisnici nisu na adekvatan način upoznati sa opasnostima od malicioznog softvera, načinima širenja zaraze i zaštitama od njih. Obuka korisnika je upravo jedna od organizacionih mera antivirusne zaštite. Ove mere zaštite usmerene su na smanjivanje opasnosti od malicioznog softvera nezavisno od drugih čisto tehničkih mera koje predstavljaju antivirusni alati.

Prva organizaciona mera jeste sprovođenje principa minimalnih privilegija. Svi programi na svim računarima treba da se izvršavaju sa ograničenim pravima. Ova prava treba da budu ograničena potrebama programa. Korisnici ne treba da koriste računare kao privilegovani korisnici operativnog sistema (*root, Administrator*) već samo kao obični korisnici. Administratorske privilegije treba koristiti samo kad je to neophodno. Razlog zašto je ovo bitno kod zaštite od malicioznog softvera je što maliciozni softver dobija prava izvršavanja kao korisnik koji je pokrenuo datoteku sa malicioznim kodom.

Druga organizaciona mera zaštite je izvršavanje (nepouzdanog) softvera u kontrolisanom okruženju, kao što su virtuelne mašine, *sandbox* i sl. Na ovaj način moguće je izvršiti proveru softvera i obezbediti da se ne realizuje nešto što je u suprotnosti sa bezbednosnom politikom.

Treća mera koja je zaista neophodna je posedovanje ispravnih – legalnih verzija svih bitnih programa u računaru. Ove kopije trebaju biti skladištene i čuvane na medijumima na koje se upisuje samo jednom, tako da je onemogućena izmena.[522]

Jedan od čestih puteva širenja zaraze na računarima su e-mail poruke. Kao meru zaštite potrebno je filtrirati ove poruke. Filtriranje pruža zaštitu od malicioznog softvera koji uključuje i spam i uglavnom se izvršava proverom priloga u e-mailu. Jednostavno filtriranje može se izvršiti zabranom nekih tipova priloga, kao na primer izvršnih ili komprimovanih datoteka. Ovo filtriranje se uglavnom vrši na osnovu ekstenzije, koja ne mora odgovarati stvarnom tipu datoteke. Detaljniji pristup proveri priloga je skeniranje korištenjem antivirusnih alata.

Osnovni koraci u antivirusnoj zaštiti su:

- instalacija nekod od antivirusnih alata,
- podešavanje na automatsko skeniranje svih datoteka,
- automatsko ažuriranje i skidanje antivirusne definicije,
- skeniranje hard diska nakon instalacije softvera,
- provera svih datoteka koje dolaze sa Interneta i
- skeniranje celog diska.

Osnovna mera zaštite od zlonamernog softvera pre svega treba da bude edukacija. Formiranje svesti o bezbednosti ključno je za zaštitu na Internetu, dok dobre prakse kao što je instaliranje anivirusnih paketa, postavljanje zaštitnih zidova i slično takođe igraju važnu ulogu.

7.4.1.3 Antivirusni programi

Prvi vid odbrane računara od virusa su antivirusni programi. Oni vrše konstantnu proveru podataka koji ulaze u računar i prepoznaju štetne zapise, a zatim upozoravaju korisnika na taj virus. Antivirusni programi treba da budu deo softvera na računaru i treba da su podešeni tako da se aktiviraju prilikom uključivanja računara, i neprekidno posmatraju sistem u računaru. Ipak, ne postoji antivirusni program koji može da otkrije sve viruse.

Svi moderni antivirusni softverski alati imaju nekoliko komponenata: deo za proveru datotea (engl. *scan*), deo za čišćenje zaraženih softvera (engl. *clean*) i stalno aktivni deo koji nadgleda ulazno-izlazne operacije na računaru i proverava da li se možda tu kreće i neki virus (engl. *monitor*). *Scan* alatima se proverava sadržaj diska u potrazi za virusima putem skeniranja fajlova, direktorijuma ili celih diskova. Ukoliko se otkrije virus,

scan program će automatski pokrenuti *clean* deo i pokušati da očisti datoteku. Čišćenje se obavlja tako što se unutar zaražene datoteke briše kod virusa. Monitor programe, većina antivirusnih programa instalira da se automatski pokreću po podizanju operativnog sistema na računaru. Kompanije koje prave i razvijaju ove programe su *Panda*, *Sophos*, *Symantec*, *Kaspersky* i dr. Najpopularniji antivirusni programi su: *Norton Antivirus*, *Sophos* antivirus, *NOD 32*, *Panda* antivirus *Titanijum*, *AVG* Antivirus, *McAffeee* i dr.

Preporuka je da se nikada ne koriste dva antivirusna softverska alata paralelno koji se automatski aktiviraju, jer može doći do sukoba između njih i do usporavanja pa čak i blokade računara. Neophodno je redovno obnavljanje antivirusa (engl. *update*) novim definicijama virusa.

7.4.2 Firewalls zaštita

Zaštita računarske mreža od napada zahteva uvođenje većeg broja bezbednosnih mera koje mogu obuhvatati korišćenje zaštitne barijere – *firewall*, *proxy* servera, demilitarizovane zone (DMZ) i sistema za detektovanja napada (IDS). [523]

Nijedna mreža, bez obzira kako je obezbeđena, nije u potpunosti bezbedna. Bezbednost mreže je veća ako potencijalni napadač mora da uloži više napora kako bi ugrozio mrežu. Kao rešenje nameće se stvaranje što više prepreka potencijalnom napadaču. Mrežna barijera odnosno *firewall*, predstavlja branu koja štiti računarsku mrežu od spoljnih slučaja, kao i od uvida u privatne podatke. Nije redak slučaj da je to i ruter posebne namene koji odvaja neku lokalnu mrežu (ili sistem lokalnih mreža) od ostatka Interneta. [524] *Firewall* u stvari predstavlja mrežni čvor. On može biti poseban uređaj ili program na čvoru. Na osnovu bezbednosne politike koja je iskazana kroz *firewall* konfiguraciju on kontroliše mrežni saobraćaj i dozvoljava ili sprečava tok. U suštini *firewall* predstavlja tehnički preventivni bezbednosni mehanizam. [525]

Firewall primarno funkcionišu koristeći tri osnovna metoda: [526]

- filtriranje paketa,
- *Network Address Translation (NAT)*,
- proxy servisi.

Za navedene funkcije mogu koristiti namenski uređaji ili serveri. U tom slučaju vrši se filtriranje paketa saobraćaja kroz *proxy* server ili se *proxy* server mora nalaziti van unutrašnje mreže, bez zaštite koju pruža filtriranje paketa. Obe metode su opasnije od upotrebe samo jednog *firewall* proizvoda koji obavlja sve bezbednosne funkcije u isto vreme. Većina *firewall* realizuje dva podjednako važna bezbednosna servisa: šifrovana autentifikacija i virtualno privatno umrežavanje (VPN). Neki *firewall*-ovi obezbeđuju dodatne servise skeniranje virusa i filtriranje prema sadržaju. Vremenom dodavane su još neke nove funkcionalnosti kao što su: praćenje stanja veze (engl. *stateful firewall*), virtuelne privatne mreže (engl. *Virtual Private Network, VPN*), sistemi za detekciju napada, provera autentičnosti komunikacije i virtuelni *firewall*. [527]

Obzirom da *firewall* povezuje dve različite mreže (unutrašnju/lokalnu i spoljašnju) i prosleđuje pakete iz jedne u drugu, može ga smatrati ruterom, što zapravo nije njegova osnovna funkcija. Osnovni zadatak mu je sprečavanje da neki sadržaji budu prosleđeni u lokalnu mrežu (koju štiti) i/ili iz te mreže. To je uređaj koji blokira pristup korisnicima koji se nalaze van mreže koju nadgleda *firewall*. U većini slučajeva predstavlja kombinaciju softvera i hardvera koje sa e šeme i pravila koja klasifikuju željeni i neželjeni saobraćaj u mreži. Svi *firewall* dele zajednički atribut: mogućnost da diskriminišu ili mogućnost da

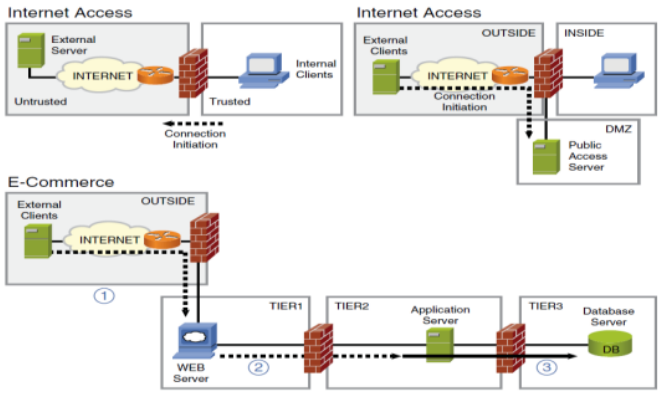
odbiju pristup koji se bazira na IP adresi. [528]

Firewall se može posmatrati kao filter koji odbacuje sve one pakete koji su naslovljeni na definisanu IP adresu lokalne mreže i/ili neki TCP port. Filtriranje komunikacije vrši se sa ciljem kontrole pristupa računarima i sadržajima lokalne mreže, ali i sa ciljem sprečavanja da se iz lokalne mreže šalje neki sadržaj. Jedna od uloga *firewall*-a u kompanijama je i da zaposlenima eventualno ograniči pristup Internetu, kao i da se dolazeći zahtevi sa Interneta usmere na one sadržaje intraneta koji ne sadrže nikakvu poslovnu tajnu. Kao rezultat *firewall* rešava problem bezbednosti tako što onemogućuje svaku komunikaciju s lokalnom mrežom za koju se proceni da bi mogla biti štetna. [529]

Firewall možemo podeliti na dve osnovne klase: *firewall* koji se koriste kao filteri i *firewall* zasnovani na primeni *proxy*.

Najčešći tip *firewall* je *network level firewall* baziran na ruterima koji odlučuju ko i šta može da pristupi mreži. Takav način obrađivanja podataka prihvata se putem tehnike koja se zove *packet filtering* koji proučava pakete koji dolaze do rutera izvan mreže. *Firewall* koji se koriste kao filteri (engl. *filter-based*) sadrže tabelu adresa i portova na osnovu koje se utvrđuje koji će se paketi proslediti, a koji odbaciti.

Proxy se nalazi između klijenta i servera i stavljajući se u položaj klijenta poprima ulogu servera dok stavljajući se u položaj servera poprima ulogu klijenta. *Proxy* vrši skladištenje raznih sadržaja (podataka, upita i odgovora) koji se često razmenjuju u okviru komunikacije između klijenta i servera. Ovaj server se obično kombinuje zajedno sa *firewall*-om i služi za keširanje web sadržaja. U tom pogledu, *proxy* server se može posmatrati kao *firewall*, gde je keširanje sadržaja druga prednost, koja pruža efikasniji rad. [526]



Slika 59. *Klasična topologija „firewall"*
Izvor: [526]

Prilikom dizajniranja zaštite mreže prvo pitanje koje se nameće je vrsta *firewall*-a. Drugo pitanje je arhitektura, odnosno raspored (lokacija) u mreži. Najčešći raspored je sa spoljašnjim i unutrašnjim *firewall*-om, kao i DMZ između njih. U zavisnosti od željenog toka informacija i bezbednosne politike koriste se različiti rasporedi. Još neke od često korišćenih arhitektura su: [530][531]

- sistem u dve mreže (engl. *Dual-Homed*),
- arhitektura sa čvorom za pregled (engl. *Screened Host*) i
- arhitektura sa mrežnim segmentom za pregled (engl. *Screened Subnet*). [531]

Glavni cilj *firewall*-a je da mrežu učini nevidljivom ili u krajnjem slučaju nedostupnom svima koji nemaju autorizovani pristup. Sa teorijskog aspekta, *firewall* je najstrožija bezbednosna mera koja može da se implementira, mada postoje diskusije po ovom pitanju. Neka zapažanja govore da je korišćenje nepraktično u okruženjima gde korisnici zavise od distribuiranih aplikacija. Zbog primene strogih bezbednosnih pravila, takva okruženja postaju sporija, jer dobijanjem bezbednosti gubi se funkcionalnost. Dodatni problem predstavljaju uska grla mrežnog okruženja, zbog autorizacije procesa i bezbednosnih mera. Međutim, i takvi uslovi su prihvatljivi ako je *firewall* pouzdan u radu. Pre izgradnje potrebno je realizovati ozbiljna istraživanja kojima se prvo treba upoznati mrežno okruženje, zbog potrebe usklađivanja velikog broja mrežnih uređaja da međusobno komuniciraju bez problema. Tako nešto postiže se automatizacijom procesa ili ljudskom interakcijom.

7.4.3 IDS/IPS zaštita

Svakog dana pronalaze se novi načini upada u ciljane sisteme, što uvećava i broj problema zbog napada od zaposlenih u kompaniji kojoj mreža pripada i koji legalno koriste pojedine delove sistema. Motivi takvih napadača u pokušajima da ugroze bezbednost sistema su različiti. [532] Odgovor na ove potrebe predstavlja pojava sistema za detekciju upada u mreže (engl. *Intrusion detection System, IDS*) i sistema za prevenciju upada u mrežu (engl. *Intrusion Prevention Systems, IPS*). [533] Nezavisno od toga koliko kompanija raspolaže modernom i kvalitetnom bezbednosnom odbranom, ona neprekidno mora biti u toku sa događanjima, novim otkrivenim ranjivostima sistema i napadima, ali i novim alatima koje napadači zloupotrebljavaju u svojim napadima na sisteme žrtve. [534]

7.4.3.1 IDS zaštita – Sistem za detekciju upada

Upad u sistem možemo opisati kao skup akcija koje pokušavaju da ugroze poverljivost, integritet ili dostupnost resursa sistema. [535] Upadi u sistem predstavljaju napade koje preventivne kontole bezbednosti nisu zaustavile. [536]

Ciljevi upotrebe sistema za detekciju upada su: [537]

- otkrivanje poznatih i nepoznatih upada; izazvanih spolja ili unutar sistema,
- pravovremeno otkrivanje upada u vremenu koje je blisko realnom,
- prikazivanje rezultata analize u jednostavnom lako razumljivom formatu koji omogućavaju da se utvrdi da li je zaista došlo do upada ili ne, i
- tačnost.

Sistem za detekciju upada – IDS (engl. *Intrusion detection System, IDS*), predstavlja jednu od tehnologija koja omogućava podizanje stepena bezbednosti sistema. Sistem proverava dolazeći i/ili odlazeći saobraćaj i vrši identifikaciju sumnjivih šablona koji mogu da ukažu na napad na mreži ili računarski sistem ili da uopšte ugroze ceo sistem. Upadi u sistem ili mrežu izvode se na različite načine: pomoću zlonamernih softvera, eksploatacijom propusta nastalih usled prekoračenja bafera u aplikacijama, slanjem paketa koje mrežna barijera propušta, a mogu i da iskoriste ranjivost neke aplikacije ili lažiranjem IP adrese. Anderson je definisao upad kao svaki neovlašćeni pokušaj da se pristupi i manipuliše podacima, da se oni izmene ili unište, ili da se sistem učini nepouzdanim ili neupotrebljivim. [538] Ipak, prvu formalnu specifikaciju modela sistema za detekciju upada dala je Denning [539] gde je objasnila da je metoda otkrivanja upada zasnovana na otkrivanju neuobičajenih događaja i predložila automatizaciju procesa.

U zavisnosti od kriterijuma klasifikacija sistema za detekciju upada može se izvršiti

na više načina. Prema kriterijumu šta se detektuje razlikujemo: [540][541]

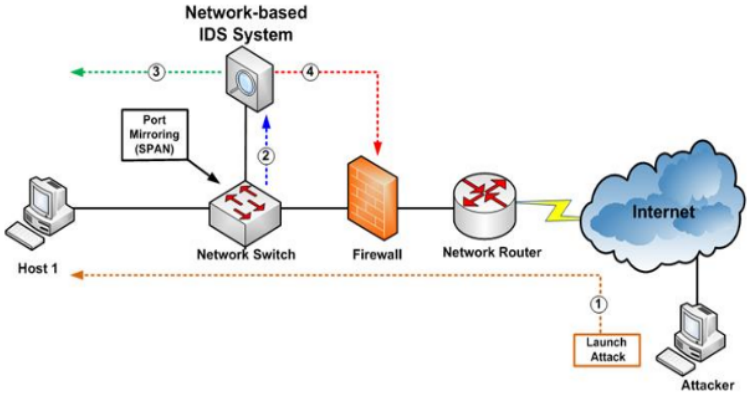
- detekciju zloupotreba (engl. *misuse intrusion detection*) i
- detekciju anomalija (engl. *anomaly intrusion detection*). [542]

Problem sa sistemom za detekciju zloupotrebe je taj što on ne može da otkrije nove tipove napada. Sistem se zasniva na poznatim uzorcima – šablonima ili oznakama poznatih napada. U poređenju sa frekvencijom smišljanja novih tipova napada, šabloni se obično retko ažuriraju. U međuvremenu sistem je ranjiv i otvoren prema novim tipovima napada i zloupotrebama.

Sistem za detekciju upada (engl. *Intrusion Detection System, IDS*) zasnovan je na prikupljanju kopija saobraćaja na određenom mestu u mreži na osnovu kojih može da alarmira i obavesti administratora o tome da je potencijalni napad u toku. [543] Informacije se prikupljaju sa čitavog niza mrežnih i računarskih izvora i analiziraju u cilju otkrivanja eventualnih nedozvoljenih aktivnosti i zloupotreba. On to radi analizom prikupljenog saobraćaja koja je slična antivirusnim programima. To zapravo znači da on poseduje bazu sa potpisima (engl. *singature*) poznatih napada i ukoliko se određeni saobraćaj poklapa sa potpisom pretpostavlja da je napad u toku. Nije retka pojava napada čiji potpis nije poznat sistemu i u tom slučaju se prati odstupanje od normalnog ponašanja sistema (engl. *baseline*). Potrebno je da sistem nauči šta je normalan – uobičajen saobraćaj kroz određeni vremenski period za šta je potrebno minimalno 30–60 dana. [544]

Tri osnovne komponente čini IDS (slika 60):

- baza potpisa (engl. *signatures*),
- senzor i
- menadžment konzole – sistema za upravljanje IDS.



Slika 60. *Implementacija IDS uređaja u računarskoj mreži*
Izvor: [544]

Na osnovu područja u kome rade, odnosno gde je IDS smešten razlikujemo:

- IDS smeštene na računaru (engl. *Host based IDS, HIDS*) i namenjene za analizu mrežnog saobraćaja koji je usmeren ka računaru na kome je postavljen IDS.
- Mrežni IDS (engl. *Networks based IDS, NIDS*) koji svoj rad zasnivaju na praćenju mrežnog saobraćaja koji teče kroz čvor – senzor. Mogu se implementirati i u ruterima, pristupnim tačkama bežičnih mreža i druge mrežne komponente, a mogu se naziti i u zasebim uređajima kao što su senzori za

otkrivanje upada. [545][546]

- aplikativni IDS smešten je u aplikaciji i štiti tu aplikaciju. Sama aplikacija odlučuje o čemu će izvestiti aplikativni IDS. [540]

Na osnovu trenutka u kome se upad dešava ovi sistemi klasifikuju napade na sledeći način: napadi u realnom vremenu (engl. *real time*) i naknadne napade (engl. *after the fact, post-mortem*). [540] Po tipu reakcije na napad, IDS sistemi se dele na pasivne i reaktivne.

Sistemi za detekciju upada – IDS (engl. *Intrusion Detection Systems, IDS*) sposobni su da izvrše razdvajanje mrežnog saobraćaja na dozvoljen i nedozvoljen. Nemoćni su u slučaju šifrovanog mrežnog saobraćaja, jer ne mogu da vrše analizu sadržaja mrežnih paketa i na osnovu sprovedene analize spreče zlonamerne aktivnosti u realnom vremenu. Problem javlja i kod komutiranih mreža (engl. *switched networks*) gde treba da se postavi veliki broj agenata koji bi omogućili praćenje mrežnog saobraćaja na svim segmentima mreže. Alati IDS mogu ukazati na lažne napade na sistem, čime otežavaju praćenje i nadgledanje saobraćaja i aktivnosti u mreži. [547][532]

Najjednostavniji sistemi za detekciju upada IDS su:

- monitori dnevničkih datoteka (eng. *Log File Monitors*),
- monitor integriteta (engl. *integrity monitor*),
- skeneri potpisa (engl. *signature scanners*).

Osnovna prednost im je što ne usporavaju mrežni saobraćaj. Analizu mrežnog saobraćaja moguće je izvršavati na računaru koji je posebno namenjen samo za prepoznavanje i praćenje napada na određene računare – aplikaciju. Osnovni nedostatak IDS uređaja leži u visokom stepenu generisanih alarma. [548] Tipičan mrežni saobraćaj sadrži veliki broj neispravnih paketa za koje IDS može samo da generiše notifikacije, iako bi bilo dovoljno odbacivati takve pakete bez obaveštavanja. Sa druge strane, IDS je izložen manjem riziku da i sam bude meta napada, jer se ne nalazi na primarnoj putanji komunikacije. I u slučaju prekida njegovog rada neće doći do problema u komunikaciji između legitimnih korisnika i servisa koji se nalaze na unutrašnjem delu mreže. [549] Postoje još neki nedostaci IDS sistema kao što su: detekcija bez sprečavanja, vremenski raskorak između napada i detekcije, lažne dojave, velike količine dnevničkih zapisa o napadima, izostanak detekcije novih vrsta napada.

Zbog ovih nedostataka važno je pomeriti nivo bezbednosti sa detekcije upada na nivo njihove prevencije. To je i bio razlog za pojavu i razvijanje sistema za prevenciju upada koji omogućavaju preventivno delovanje kada su u pitanju računarski napadi i izbegavanje nastanka štete koja bi bila prouzrokovana tim napadima.

7.4.3.1 IPS zaštita – Sistem za prevenciju upada

Sistemi za prevenciju upada (engl. *Intrusion Prevention System, IPS*) smatraju se sledećom generacijom sistema za detekciju upada. Najčešće nije dovoljno samo izvršiti detekciju izvedenih napada već je za održavanje bezbednosti u računarskom i mrežnom okruženju potrebno implementirati i sisteme za prevenciju upada. [550]

Sistem IPS predstavljaju integraciju postojećih bezbednosnih tehnologija u jedan celovit sistem. Jedan od osnovnih zadataka IPS je da sprečava poznate i nepoznate napade na računarske sisteme. IPS sadrži i algoritme za otkrivanje napada na osnovu definisanih bezbednosnih politika i anomalija u sistemu. Pored detekcije upada i izveštavanja, od IPS se očekuje da obezbedi automatizovani odgovor kojim će se sprečiti dalji tok napada. [551]

Osnovne funkcionalnosti IPS su:

- identifikacija neovlašćenih aktivnosti na osnovu potpisa,
- identifikacija neovlašćenih aktivnosti na osnovu detektovanih anomalija,
- vođenje evidencije i/ili slanje upozorenja u realnom vremenu administratorima zaduženim za bezbednost,
- prikupljanje forenzičkih podataka o detektovanim napadima,
- sprečavanje napada. [552][553]

Jedan od najvažnijih ciljeva svakog IPS je da omogući jednostavnu skalabilnost, ali da proširivanjem kapaciteta, distribucijom procesne logike ne naruši ispravnost algoritma za detekciju. Imajući u vidu princip rada IPS, mogu se svrstati u dva osnovna tipa:

- IPS sistemi smešteni na računaru (engl. *host based IPS, HIPS*),
- mrežni IPS sistemi (engl. *network based IPS, NIPS*).

Često je potrebno kombinovati IPS alate za zaštitu mreža i sisteme za sprečavanje neovlašćenih aktivnosti na klijentskim računarima [554] jer oni prikupljaju podatke o aktivnostima unutar sistema analiziraju ih i prepoznaju upade.

7.4.3.1.1 HIPS – IPS za zaštitu pojedinih računara

Programski alati za prevenciju upada na pojedinačnim računarima (engl. *host based IPS, HIPS*) predstavljaju alat koji se realizuje kao aplikacija instalirana na računaru (klijent ili server) koja funkcioniše kao agent koji obrađuje različite bezbednosne politike pročitane iz konfiguracione datoteke i može biti smeštena na centralnom upravljačkom serveru. Njegovom primenom olakšava se održavanje i praćenje čitavog sistema. [555]

Za implementaciju HIPS koristi se nekoliko metoda. Prvi koncept rada HIPS je da nakon instalacije, HIPS može određeno vreme da prati rad svih procesa na računaru i skladištiti ih u svoju bazu uobičajenih aktivnosti računara. Nakon što je „naučio" uobičajene aktivnosti u radu računara, HIPS je u stanju da prepozna sve procese koji se ponašaju drugačije od standardnog ponašanja tako da ih može detektovati i dojaviti da se radi o nedopuštenim aktivnostima ili ih pak ukloniti. U ekstremnim uslovima sa mreže se uklanja i ugroženi računar, kako bi se sprečilo širenje na ostalim računarima u mreži. [556] Drugi koncepti rada HIPS uključuju integraciju sa *firewall*-om koji je instaliran na istom računaru. Tako se ostvaruje zaštita računara na mrežnom nivou te se potencijalno zlonamerni paket odbacuje pre nego što uopšte dospe do aplikacije prema kojoj je usmeren. Moguće su i varijante zasnovane na traženju različitih zlonamernih kombinacija asemblerskih naredbi koje bi mogle uzrokovati prepisivanje buffera (engl. *buffer overflow*) i slično.

HIPS sistemi obezbeđuju kompanijama dodatni nivo zaštite jer omogućavaju detekciju najnovijih upada za koje pravila još nisu definisana. Ovakav pristup posebno je važan za otkrivanje i blokiranje napada nultog dana koji se zasnivaju na eksploataciji najnovijih bezbednosnih propusta pre nego što su objavljene odgovarajuće bezbednosne zakrpe. Važno je i to da će HIPS blokirati sve aktivnosti za koje se smatra da odstupaju od legitimnog ponašanja definisanog parametrima programa.

I HIPS ima svoje prednosti i nedostatke. Prednosti su mu:

- zaštita od napada nultog dana na sistem,

- smanjenje obaveza zaposlenih koji su odgovorni za bezbednost,
- smanjenje troškova održavanja sistema i
- mogućnost implementacije u aplikacije koje su u razvoju.

Nedostaci HIPS sistema su:

- troškovi implementacije (sistem zahteva agenta za svaku radnu stanicu),
- relativno dug period implementacije i konfiguracije (obučavanje zaposlenih),
- izazivanje problema u radu aplikacija (ako je sistem loše konfigurisan),
- neophodnost ispitivanja svake nove aplikacije u interakciji sa HIPS pre uvođenja,
- ne saniraju infekcije sistema koje su se već pojavile.

7.4.3.1.2 NIPS – IPS za zaštitu mreže

Mrežni IPS sistemi (engl. *network based IPS, NIPS*) kombinuju funkcionalnosti standardnih NIDS i mrežnih barijera sa dodatnim metodama sprečavanja zlonamernih aktivnosti. NIPS ima dve mrežne kartice, jednu koja je namenjena unutrašnjoj mreži, i drugu koja je namenjena vezivanju na spoljašnjoj mreži. Kada se paket pojavi na bilo kom mrežnom okruženju, IPS ih analizira i odlučuje da li oni predstavljaju pretnju. Takav način rada IPS je preventivan za razliku od IDS koji prosleđuje pakete pa tek onda kontroliše da li paket predstavlja pretnju. [557]

Neki IDS nakon što ustanove nelegitimnost uspostavljene veze, mogu je i prekinuti. To neće uticati na to da paketi koji su stigli pre saznanja o nelegitimnosti veze ipak budu prosleđeni na svoja odredišta gde mogu uzrokovati probleme u radu. Sve funkcionalnosti mrežne barijere zadržane su i u NIPS, kao što to su *stateful inspection* tehnologija koja se zasniva na kontinuiranom praćenju i analizi pojedinih segmenata veze koji prolaze kroz *firewall*, kako bi se na bazi njih u realnom vremenu mogle donositi pravilne odluke o filtriranju paketa. Glavno unapređenje koje je implementirano kod NIPS je dubinska analiza sadržaja paketa (engl. *Deep Packet Inspection*) u realnom vremenu. Pomoću dubinske analize sadržaja paketa u realnom vremenu, NIPS je u mogućnosti da detektuje prikrivene napade prvenstveno usmerene na web, e-mail i DNS servere. Obzirom da se unutar jednog mrežnog paketa ne može otkriti zlonamerni sadržaj, NIPS prikuplja veće količine mrežnih paketa kako bi vršio grupnu obradu nad njima. Paketi se analiziraju, ponovo sastavljaju i u slučaju nepronalaženja sumnjivog zlonamernog sadržaja prosleđuju na odredište na koje su paketi i usmereni. Takvim radom NIPS dobija potpunu sliku o podacima koji su primljeni, ali i primenjuje proceduru koju definiše korisnik. NIPS može da u ponovnom slanju paketa ispravi nepravilnosti u poretku paketa eventualno nastale u prenosu ili koje su namerno izazvane od strane napadača.

Prednosti NIPS sistema su:

- blokiranje širenja crva bez zaustavljanja legitimnog mrežnog saobraćaja,
- štiti od novih napada i
- smanjuje troškove otklanjanja posledica incidenata.

Nedostaci NIPS sistema su:

- troškovi uvođenja,

- predstavljaju jednu tačku otkaza sistema (engl. *single point of failure*),
- isplativost investicije,
- ugrožavanje bezbednosti sve češće prolazi neprimećeno tako da rukovodioci kompanija nisu svesni štete koju trpe dok to ne postane očigledno i
- potreba za podizanje svesti i obrazovanje. [558]

Ovakvi sistemi štite računarske mreže i/ili pojedinačne računare podižući bezbednosnu zaštitu na viši nivo omogućavajući tako pravovremenu detekciju i sprečavanje zlonamernih aktivnosti. Prilagođeno upozoravanje olakšava administratorima kontrolu i upravljanje sistemom. Ipak, pred ove sisteme postavljaju se visoki zahtevi. Jedan od osnovnih je zahtev za održavanjem visokih performansi sistema. Za implementaciju sistema koji bi zadovoljio sve postavljene zahteve trebalo bi obezbediti visoka finansijska sredstva.

7.4.3.1.3 Metode detekcije napada

Za detekciju napada postoji više metodologija. Obično se više vrsta detekcije kombinuju u cilju postizanja preciznisnosti i detekcije šireg dijapazona pokrivanja anomalija. Razlikujemo nekoliko metodologija. [558]

Sugnature-based, metoda bazira se na poređenju poznatih pretnji, kako bi se utvdio incident na željenom događaju. Predstavlja efikasan pristup za detekciju poznatih pretnji, ali neefikasan u detekciji nepoznatih pretnji ili složenih varijanti poznatih pretnji.

Anomaly-based detection, u cilju otkrivanja anomalije zasniva svoju funkcionalnost poređenju posmatrane aktivnosti sa uobičajenim aktivnostima na mreži. Formira se profil tipičnih aktivnosti tokom vremena. Nakon toga IPS poredi karakteristike konkretne aktivnosti sa formiranim pragom odlučivanja, na osnovu formiranih tipičnih profila. Ovaj vid detekcije je veoma efikasan kada se radi o predhodno nepoznatim pretnjama. [558]

Stateful protocol analysis je metoda zasnovana na već određenim profilima prihvatljivih protokolarnih aktivnosti u svakoj fazi aktivnosti protokola, sa posmatranim događajem u cilju identifikacije devijacije. *Stateful* analiza pruža mnoge efikasne mogućnosti za detekciju, a koje nisu prisutne u predhodne dve metode. [558]

7.4.3.1.4 Karakteristike IPS nove generacije

Sistemi nove generacije IPS, obezbeđuju neke karakteristike, olakšavajući primenu, pametnijim načinom rada u svrhu dinamičke odbrane. To su pre svega automatizovana procena uticaja, automatsko fino podešavanje i praćenje identiteta korisnika. [558]

Automatizovana procena uticaja karakteristična je po tome što jednom detektovan napad na bilo kom serveru u mreži će automatski biti prosleđen svim ostalim serverima čime će se u potpunosti redukovati svi potencijalni budući događaji koje bi taj napad izazvao u čitavoj mreži. [558]

Vreme koje je potrebno da se poveže korisnik sa bezbednosnim događajem može biti smanjeno sa jednog sata na manje od jedne sekunde. Postavlja se pitanje kakva je korist neke IP adrese za uređaj krajnjeg korisnika ako ne znamo ko je napadnut ili ko krši IT politiku firme u odnosu na bezbednosni događaj ili događaj usklađenosti. [558]

7.4.4 Slojevita zaštita

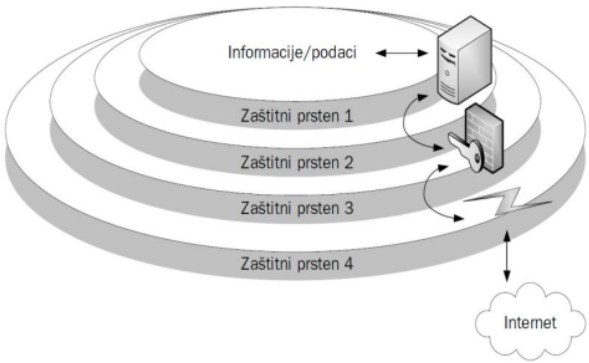
Kako bi se kompanije adekvatno zaštitile od potencijalnih opasnosti i raznovrsnih napada kojima se ugrožavaju različiti servisi i resursi u okviru informacionih sistema,

predlaže se implementacija arhitekture sistema zaštite koja se zasniva na formiranju zaštitnih slojeva (ili prstenova) oko sistema. Zaštita se sastoji od mehanizama koji se primenjuju na 3 i nezavisna bezbednosna nivoa sa ciljem ograničavanja i smanjenja mogućih šteta tako što eventualno u2ožavanje jednog nivoa ne može kompromitovati ostale bezbednosne nivoe arhitekture sistema. Korisnik sistema koji prolazi kroz slojeve zaštite mora zadovoljiti dodatne bezbednosne mehanizme koji zadržavaju napadača ili minimizuju njegovu mogućnost pristupa kritičnim resursima kompanije. [544] 71

U slojevitom pristupu potrebno obezbediti kombinaciju bezbednosnih mehanizama i tehničkih rešenja koja obuhvataju dovoljno širok opseg bezbednosnih zahteva. Uz to, treba onemogućiti da probijanje jednog sloja ima nesagledive posledice po bezbednost čitavog sistema. Verovatnoća da budu probijeni svi slojevi mnogo je manja od verovatnoće probijanja jednoslojne zaštite. [544] 3

Mehanizmi zaštite informacionog sistema kompanije mogu se sastojati od primenjenih mehanizama na sledeća tri nivoa:

- zaštita „s kr3a na kraj" (engl. *end-to-end security*) na aplikativnom nivou, gde se globalno obezbeđuje:
  - provera izvornosti korisnika servisa kako u smislu komunikacije (engl. *end-user authentication*) tako i opciono u smislu kontrole pristupa informacionom sistemu (engl. *access control*),
  - zaštita integriteta podataka koji se prenose,
  - zaštita od mogućnosti naknadnog poricanja odgovornosti za poslate podatke i
  - zaštita tajnosti podataka.
- zaštita na transportnom nivou,
- zaštita na mrežnom IP nivou. [544]



Slika 61. *Slojevita zaštita*
Izvor: [544]

Slojevitu zaštitu ilustrovaćemo na primeru četiri prstena (slika 61). Razlikujemo:

- zaštitini prsten 4 (spoljašnji sloj) predstavlja granicu između sistema i spoljašnjeg sveta (Internet),

- zaštitni prsten 3 (treći zaštitni sloj) štiti sistem od mreže u kojoj se nalazi i sadrži mehanizme PKI (infrastruktura javnih ključeva), VPN i mrežne barijere (*firewall*),
- zaštitni prsten 2 (drugi sloj) implementira CIA koncepte koristeći mehanizme na sistemskom nivou i
- zaštitni prsten 1 (unutrašnji sloj) štiti same informacije i podatke koji se čuvaju na sistemu. [544]

7.4.4.1 Zaštita na aplikativnom nivou

Da bi se realizovali mehanizmi zaštite na aplikativnom nivou u okviru informacionog sistema kompanije, moguća je primena digitalnog potpisa i digitalne koverte (engl. *envelope*), na bazi pametnih kartica za korisnike. Realizacija zaštite na aplikativnom nivou podrazumeva primenu odgovarajuće kriptografske biblioteke kako na klijentu, u okviru odgovarajuće klijentske aplikacije (*standalone*) ili Internet pregledača, tako i na odgovarajućem web ili aplikativnom serveru. Ovakvo rešenje treba da ima sledeće kriptografske karakteristike.

- Mezanizmi zaštite na aplikativnom nivou treba da obezbede: autentičnost potpisnika, zaštitu integriteta datoteka, obezbeđenje neporečivosti i zaštitu tajnosti podataka.
- Upoterbljavaju se tehnologije digitalnog potpisa i digitalne koverte.
- Univerzalnost u odnosu na pametne kartice i čitače pametnih kartice.
- Klijentska aplikacija sa ugrađenom kripto kontrolom koja obezbeđuje proveru autentičnosti korisnika na osnovu njegove pametne kartice i odgovarajućeg PIN pre nego što se omogući korišćenje same aplikacije, tj. aplikacija ne može da se startuje bez korišćenja odgovarajuće pametne kartice ovlašćenog korisnika.
- Zasniva se na kriptografskim funkcijama koje se izvršavaju na pametnoj kartici: digitalni potpis (tj. *RSA private key encryption*) i dešifrovanje simetričnog ključa kod digitalne koverte (engl. *digital envelope retrieval*).
- Zasnica se na PKCS standardima za zaštitu: PKCS#1 za digitalni potpis i digitalnu kovertu, PKCS#7 za format zaštićenih podataka i PKCS#11 standardni interfejs za pristup pametnim karticama.
- Aplikacija treba da bude standardizovana u smislu formata digitalno potpisanih i šifrovanih podataka.
- Aplikacija pri implementaciji bezbednosnih mehanizama treba da koristi standardne načine pristupa pametnim karticama: *CSP* (engl. *Cryptographic Service Provider, CSP)* i PKCS#11 biblioteke.
- Klijentska *standalone* aplikacija i web aplikacije, treba da pruže: izbor sertifikata potpisnika (koji stoje u *Personal Store*), prikaz informacija o podacima koji se digitalno potpisuju pre samog potpisivanja, prikaz informacija o rezultatima digitalnog potpisivanja i/ili šifrovanja datih podataka i prikaz informacija o rezultatima uspešne ili neuspešne verifikacije digitalnog potpisa i/ili uspešnog ili neuspešnog dešifrovanja datih podataka.
- Klijentska i serverska kripto komponenta treba da ima sledeće karakteristike:
  - asimetrični algoritmi – RSA algoritam (koji se izvršava na pametnoj

kartici) sa dužinom asimetričnog ključa od 2048 bita,

- hash algoritmi – SHA-1, SHA-224, SHA-256, SHA-384 ili SHA-512,
- simetrični algoritmi – 3DES algoritam sa dužinom ključa od 168 bita ili AES algoritam sa dužinama ključa od 128, 192 ili 256 bita.

- Aplikaciju stalno treba nadograđivati kako novim algoritama, ali i menjati one algoritme za koje je utvrđeno da su kriptografski slabi za korišćenje.
- Aplikacija je otvorena za eventualnu ugradnju privatno razvijenih simetričnih algoritama i verifikovanih od strane nadležne institucije za poslove kriptozaštite u zemlji, ukoliko postoje zahtevi za to.
- U okviru aplikacije treba omogućiti funkciju verifikacije digitalnog potpisa podataka koji se sastoji od sledeća dva koraka:
  - provera digitalnog potpisa podataka na osnovu javnog ključa iz digitalnog sertifikata potpisnika,
  - provera validnosti digitalnog sertifikata.

U okviru mehanizama zaštite na aplikativnom nivou treba integrisati i odgovarajuću proceduru *challenge-response* jake autentifikacije korisnika na aplikativnom nivou. Alternativa je da se u tu svrhu upotrebi procedura klijentske i serverske autentikacije u okviru SSL protokola zaštite na transportnom nivou.

7.4.4.2 Zaštita na transportnom nivou

U cilju implementacije mehanizama za zaštitu na transportnom nivou, treba primeniti standardni *SSL* (engl. *Secure Sockets Layer, SSL*) protokol između korisnika i web servisa. Moguće su sledeće osnovne konfiguracije SSL protokola:

- SSL protokol sa serverskom autentifikacijom ili
- SSL protokol sa klijentskom i serverskom autentifikacijom zasnovan na digitalnim sertifikatima i pametnim karticama korisnika.

Informacioni sistem kompanije treba da implementira SSL protokole sa klijentskom i serverskom autentifikacijom. Autentifikaciju korisnika informacionog sistema kompanije, treba realizovati na transportnom nivou sa visokim stepenom autentifikacije korisnika na bazi SSL protokola koji se zasniva na primeni pametnih kartica korisnika i na njima izdatih digitalnih sertifikata. Tako se postiže da samo klijenti sa pametnim karticama i odgovarajućim digitalnim sertifikatima mogu pristupiti datom web serveru, a samim tim i da izvršavaju odgovarajuće procese u okviru informacionog sistema kompanije.

7.4.4.3 Zaštita na mrežnom nivou

Zajedno sa SSL protokolom na transportnom nivou, mogu se koristiti i kriptografski mehanizmi zaštite na mrežnom nivou koji se zasnivaju na *IPSec* protokolu zaštite i uspostavljanju virtuelnih privatnih mreža (VPN). VPN mreže se najčešće zasnivaju na čistom *IPSec* protokolu zaštite ili na kombinacijama *PPTP/IPSec* ili *L2TP/IPSec* protokola.

Ako poslovne jedinice ne komuniciraju putem korporativne mreže u vlasništvu kompanije, neophodno je uspostaviti VPN tunel na bazi *IPSec* protokola *site-to-site* tipa. Kada eksterni ili interni korisnici pristupaju udaljeno ili od kuće, neophodno je upostaviti *PPTP/IPSec* ili *L2TP/IPSec* putem odgovarajućeg VPN klijenta na strani korisnika i

odgovarajućeg VPN koncentratora na strani kompanije. Terminaciju VPN tunela u ovom slučaju uglavnom treba vršiti na eksternom interfejsu *firewall* uređaja.

U okviru informacionog sistema kompanije uglavnom se primenjuje *IPSec* protokol na bazi digitalnih sertifikata čvorova u računarskoj mreži (ili između klijenta i VPN servera). VPN mreža zasnovana na *IPSec* protokolu, može se uspostaviti između dva rutera ili rutera i *firewall*-a, ili između VPN klijenta i VPN koncentratora (ruter ili *firewall* uređaj) – opet na bazi digitalnih sertifikata.

7.5 Reaktivna i prediktivna zaštita

Osnovna uloga sistema zaštite je održavanje bezbednosnog stanja informacija i IKTS na prihvatljivom nivou rizika. Praksa zahteva da zaštita bude izbalansirana i komplementarna, gde se vrši zamena manje efikasnih i efektivnih kontrola sa efikasnijim i efektivnijim, dok se tehničke kontrole dopunjavaju proceduralnim kontrolama. Primena samo tehničkih kontrola predstavlja parcijalno rešenje reaktivne zaštite ili „popravku" sistema od poznatih ranjivosti i pretnji. Većina registrovanih upada u IKTS, rezultat su korišćenja poznatih ranjivosti OS ili grešaka konfiguracije, za koje su bile na raspolaganju kontrole zaštite, ali nisu implementirane. Cilj definisanja koncepta kontrola zaštite je obezbeđivanje skupova skalabilnih upravljačkih (U), operativnih (O) i tehničkih (T) kontrola za osnovni, poboljšani i visoki nivo zaštite.

7.5.1 Koncept sistema reaktivne zaštite

Koncept reaktivne zaštite je zaštita od poznatih ranjivosti i pretnji. Sistem reaktivne zaštite u većini slučajeva kasni, a nove napredne tehnike napada čine nekorisnim prethodno ažurira nedefinicije virusa. Reaktivna zaštita je tipična za većinu IDS sistema, ali ne i za savremene IDPS sisteme. [559]

U praksi najčešće dolazi do incidenata koji nisu planirani i za koje se misli da se nikada neće dogoditi. Često se sistem zaštite razvija neplanirano, kao reakcija na poslednji napad ili vanredni događaj, ili neusklađeno sa procenom rizika i potrebama, čime se stvara redundantan i skup reaktivni sistem zaštite. Primena samo T kontrola predstavlja parcijalno rešenje reaktivne zaštite, gde popravljeni sistem zadržava ranjivosti. [560]

7.5.1.1 Funkcionalni model reaktivne zaštite

Funkcionalni model sistema reaktivne zaštite sadrži sledeće faze: identifikaciju stanja zaštite, procenu rizika, planiranje i implementaciju poboljšanih kontrola zaštite, operativno održavanje, nadzor, reviziju, obuku i obrazovanje. [560][561]

Opšti funkcionalni modeli upravljanja sistemom reaktivne zaštite mogu se definisati na više načina i sa različitih aspekata. Sa metodološke tačke gledišta, upravljanje sistemom reaktivne zaštite najbolje se predstavlja procesom upravljanja rizikom u IKTS, koji obuhvata faze planiranja, izbora T kontrola, izbora modela zaštite, razvoja/akvizicije i selekcije kontrola i izrade uputstva za upravljanje rizikom/sistemom zaštite. [562]

Primeri procesa upravljanja sistemom zaštite su distribucija kriptografskih ključeva, izveštavanje o incidentu, aktiviranje/dezaktiviranje servisa zaštite, implementacija politike zaštite i sl.

Baza podataka zaštite (BPZ) predstavlja skladište relevantnih informacija za upravljanje sistemom višeslojne zaštite. U praksi, delovi BPZ mogu, ali ne moraju, biti integrisani u bazu podataka IKTS.

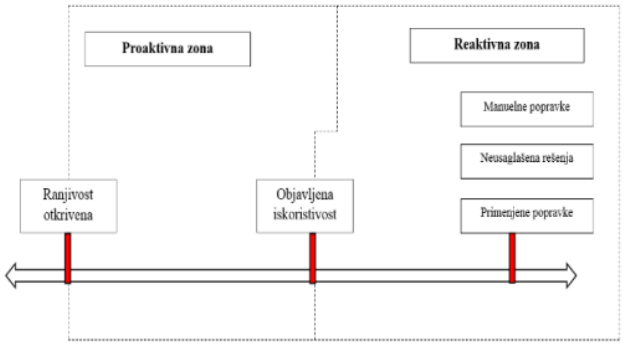
7.5.1.2 Funkcionalni model reaktivne zaštite

U sistemu reaktivne zaštite, kompanije u Internet okruženju tipično primenjuju tri moguća, u suštini reaktivna rešenja: da ne preduzimaju ništa, da primenjuju manuelne ili poluautomatizovane tehnike bezbednosnih popravki (engl. *patches*) ili da izvrše *ad-hoc* samozaštitu sa izolovanim tehničkim rešenjima na distribuiranim tačkama IKTS.

Metod „ne preduzimati ništa" najčešće se zasniva na predpostavci „da se to neće baš nama dogoditi i sl.". Ipak, pravi dokaz o postojanju pretnje obično dolazi nakon uspešno izvršenog napada sa nekim gubitkom. Slično je kada IKTS ima samo logičku mrežnu barijeru (engl. *firewall*) ili neku drugu statičku formu infrastrukturne zaštite, koja ne obezbeđuje dovoljnu zaštitu za *on-line* režim rada. [563]

Ručna i improvizovana metoda rešavanja ranjivosti predstavlja stari metod reaktivne zaštite. Teoretski je moguće pratiti sve potencijalne izvore pretnji, preuzeti sve relevantne bezbednosne popravke ranjivosti i zatim testirati i instalirati svaku od njih, na svakom potencijalno ugroženom računarskom sistemu. Ipak, potrebno je značajno vreme za identifikovanje, manuelnofiksiranje i testiranje potencijalno ranjivih RS u mreži. U odnosu na prvu opciju, ni ovo rešenje ne obezbeđuje adekvatnu strategiju zaštite.

Neusaglašena rešenja zaštite na izolovanim, distribuiranim tačkama IKTS su rešenja koja trenutno preovlađuju u svetu. Obuhvataju slojevitu zaštitu po dubini, na više nivoa i sa više različitih komponenti zaštite. Upravljanje u ovakvom sistemu je vremenski zahtevno, skupo i kompleksno. Rešenje je jednokratno, ali ne obezbeđuje koherentnu, integralnu i uniformnu zaštitu IKTS. Vremenski prozor reaktivne zone zaštite, sa različitim rešenjima i manuelnim otklanjanjem ranjivosti, nalazi se između vremena objavljivanja iskorišćavanja određene ranjivosti i manuelne popravke te ranjivosti (slika 62). [516]



Slika 62. *Vremenski prozori proaktivnih i reaktivnih sistema zaštite*
Izvor: [516]

Sve mere zaštite u reaktivnoj zoni usmerene su na reaktivno saniranje i oporavak sistema. U ovoj zoni nalaze se i različita rešenja postojećih sistema reaktivne zaštite, od kojih se većina fokusira na otkrivanje ranjivosti sistema. Administratori zaštite nemaju realne mogućnosti da selektuju kritične ranjivosti od minornih, dok običan IDS preduzima akcije, tek kada napad započne. Pored toga, za analizu incidenta podaci se ručno prikupljaju sa različitih tačaka i u raznim formatima iz log datoteka distribuiranih računarskih sistema, što znatno usporava i otežava ceo taj proces.

Manuelne i poluautomatske popravke ranjivosti sistema, danas su standardni metodi koji obezbeđuju dovoljnu, ali kontrolisanu zaštitu na prihvatljivom nivou rizika. Reaktivni sistemi zaštite troše velike resurse za planiranje, bekapovanje i oporavak sistema od, često, samo jednog napada. Rešenje je da se implementira rentabilna proaktivna

detekcija napada i IKTS štitiod poznatih i nepoznatih pretnji.

7.5.2 Koncept sistema proaktivne zaštite

Prvi korak u razvoju sistema proaktivne zaštite je korišćenje baza znanja i drugih servisa najbolje prakse zaštite, koji omogućavaju krajnjim korisnicima sopstvenu implementaciju i upravljanje zaštitom. Koncept sistema proaktivne zaštite obezbeđuje zaštitu od iskorišćavanja poznatih i nepoznatih ranjivosti, zaustavljanjem malicioznih napada na samom izvoru nastanka. [564] Obezbeđuje veću rentabilnost vremena i troškova od postojećih reaktivnih sistema. Sistem zaštite reaguje brzo i precizno nakombinovane, dinamički promenljive pretnje (DPP).

7.5.2.1 Funkcionalni model proaktivne zaštite

Metod proaktivne zaštite obuhvata mehanizme zaštite na više nivoa, sa različitim brzinama reakcije i tačnosti, sa većom ukupnom efektivnošću, redukovanim operativnim rizicima i znatno nižim troškovima razvoja, rada i održavanja. Koncept sistema DPP zaštite nudi nov proaktivni pristup, u kome se zaštita realizuje kombinacijom baza znanja, vrhunske tehnologije za proaktivnu zaštitu, procesnog pristupa i pojednostavljenog rešenja sistema zaštite. [516][564]

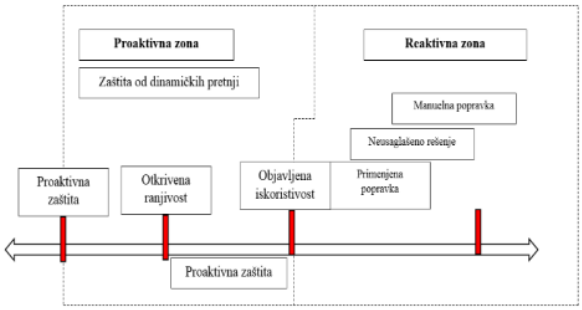
Baze znanja vodećih mreža CIRT i CERT, prikupljaju podatke o pretnjama i ranjivostima sistema i obezbeđuju ažuran bilten podataka (*X-Press Updates*), u kome detaljno opisuju brojne ranjivosti sistema. Tehnologija višeslojne proaktivne zaštite obezbeđuje automatizaciju ciklusa zaštite sa elementima ekspertnih sistema i obuhvata:

- uređaj za zaštitu (engl. *Protection Engine*),
- uređaj za zaštitu lokacije (engl. *Site Protector*),
- integrator sistema (engl. *Fusion System*) i
- modul za ažuriranje (*X-Press Updater*). [564]

Procesni pristup zaštiti i pojednostavljeni proces zaštite, bitne su komponente koncepta proaktivne DPP zaštite. Rešenja DPP zaštite upotrebljavaju jedinstveni mehanizam virtuelne zakrpe (engl. *Virtual Patch*) za automatsko fiksiranje poznatih i mogućih ranjivosti sistema. [564] Ovaj mehanizam omogućava kompaniji da u realnom vremenu, zaštiti sistem od poznatih i nepoznatih napada, često znatno ranije od zvaničnog generisanja i objavljivanja popravki za nove ranjivosti sistema. [516]

Proces proaktivne zaštite počinje sa otkrivanjem/objavljivanjem ranjivosti sistema. Potom sledi generisanje napada, koji može iskoristiti otkrivenu ranjivost sistema. Konačno, generiše se i primenjuje nova bezbednosna popravka za otklanjanje ove moguće ranjivosti. Iako je vreme od otkrivanja do iskorišćavanja ranjivosti promenljivo, popravka se često primenjuje tek kada je šteta već naneta.

U vremenu od otkrivanja do iskorišćavanja ranjivosti, nalazi se prozor proaktivne zaštite. U tački otkrivanja ranjivosti sistema aktivira se *Virtual Patch* proces, aktivira sistem za proaktivnu zaštitu i obezbeđuje zaštita i bez poznavanja informacije o iskoristivosti te ranjivosti. Zonu proaktivne zaštite DPP obezbeđuje *Virtual Patch*proces, koji štiti sistem od nepoznatih pretnji. U stvari, proaktivna zona zaštite proteže se i na zonu pre otkrivanja ranjivosti sistema (slika 63), što omogućavaju stalni procesi istraživanja i razumevanja prirode ranjivosti IKTS.



Slika 63. *Prošireni vremenski prozor proaktivne zaštite*
Izvor: [516]

Proaktivni sistem zaštite, u poređenju sa reaktivnim, postiže rentabilnije vreme analize i upravljanja rizikom, veću tačnost i brzinu detekcije kao i efektivnije sprečavanje napada. Obzirom da pretnje i ranjivosti rastu, sistem zaštite mora biti brži, precizniji i pouzdaniji. Napadačima je za efektivan napad dovoljna margina greške od 1%. Centralna platforma za DPP zaštitu, obezbeđuje znatno kvalitetniju zaštitu cele RM i smanjuje složenost, eliminiše lažne uzbune, znatno smanjuje ukupne troškove zaštite i približava se optimalnom sistemu zaštite. Proaktivni sistem zaštite zadovoljava zahteve savremenih trendova zaštite virtuelizovanog okruženja u distribuiranom Internet računarstvu (CC), mreža u razvoju, mobilnih uređaja, senzorskih sistema za fizičku zaštitu, alternativnih puteva isporuke mehanizama zaštite,upravljanja rizikom i identitetom. [564]

7.5.3 Organizacione mere zaštite

Bezbednost podataka u informacionim sistemima veoma je kompleksna i široka tema u kojoj je jasna jedino činjenica da bez kvalitetnih mera bezbednosti sistem nije moguće zaštiti u celini.

Organizacione mere zaštite su:

- politika bezbednosti informacionog sistema,
- procena rizika,
- identifikacija resursa,
- podela resursa,
- bezbednosne mere za zaposlene i
- procedure rada i odgovornosti. [564]

7.5.3.1 Politika bezbednosti informacionih sistema

Prvi korak ka potpunosti obezbeđivanja bezbednosti sistema je definisanje politike bezbednosti. Njena primarna uloga je određivanje prihvatljivosti načina ponašanja kako bi se zaštitili vrednosti informacionog sistema, uključujući opremu (engl. *hardware*), programsku podršku (engl. *software*) i podatke.

Politiku bezbednosti možemo sagledati kao pravila, smernice i postupke koji definišu način na koji se informacioni sistem čini bezbednim i kako štiti njegova tehnološka i informaciona vrednosti. Ona odgovara korisnicima šta smeju šta ne, šta su obavezni da preduzimaju i koja je njihova odgovornost. [565] Na osnovu pravila definisanih u dokumentu, ima zadatak je da obezbedi tri jedinstvena svojstva informacija:

poverljivost (tajnost), integritet i dostupnost. Bezbednosnom politikom definišu su pravila koja se odnose na: svu računarsku opremu, lica odgovorna za administraciju informacionog sistema, kao i lica koja imaju pravo pristupa.

Nakon definisanja bezbednosne politike važno je obezbediti da se pravila koja su definisana bezbednosnom politikom sprovode i poštuju. Dokument bezbednosne politike mora biti odobren od strane najvišeg rukovodstva u kompaniji, objavljen i s njim trebaju biti upoznati korisnici informacionog sistema. Politika bezbednosti informacionog sistema treba da sadrži: definicije bezbednosti informacija, njene sveobuhvatne ciljeve i delokrug, važnost bezbednosti kao osnovni mehanizam deljenja informacija, stavove rukovodstva, uz podršku ciljeva i principa informacione bezbednosti.

7.5.3.2 Procena rizika

Bitan korak pri uspostavljanju bezbednosti informacionih sistema je procena rizika. Iako je osnovni deo sistema upravljanja informacionom bezbednošću (ISMS), procena rizika tesno vezana sa kreiranjem bezbednosne politike. Proces procene rizika nije malo jednostavan, ali najlakše bi se mogao opisati kao davanje odgovora na sledeća četiri pitanja:

- Šta se može dogoditi? – događaj pretnje.
- Ako se dogodi, kolika šteta može nastati? – učinak pretnje.
- Koliko često se može dogoditi? – frekvencija pretnje.
- Koliko su tačni odgovori na prva tri pitanja?

Odgovori na ova pitanja mogu biti sa dugom listom predloga šta bi trebalo da se preduzme. Često je potrebno ova pitanja proširiti sa još tri:

- Šta se može učiniti?
- Koliko će učinjeno koštati?
- Da li je utrošeno isplativo?

Odgovori na prethodno postavljena pitanja pra balans između potreba i mogućnosti kompanija za implementaciju bezbednosnih kontrola. Kako bi se postigla ravnoteža potreb mogućnosti neke rizike je potrebno prihvatiti. Važan deo upravljanja bezbednošću je upravljanje rizikom, odnosno, uspostavljanje odnosa između ranjivosti, mogućih pretnji i posledica – uticaja na informacioni sistem. Proces upravljanja rizikom sastoji se od: identifikacije resursa, analize rizika, tumačenja rezultata i preduzimanja odgovarajućih protivmera.

7.5.3.3 Identifikacija resursa

Jedan od uslova za uspešno upravljanje informacionom bezbednošću u informacionom sistemu je identifikacija resursa. Bez precizne identifikacije resursa nema ni realizacije kvalitetne zaštite. U procesu identifikacije resursa potrebno je prebrojati sve resurse unu informacionog sistema ali i izvršiti procenu njihove relativne vrednosti za kompaniju. Na osnovu toga u procesu upravljanja rizikom, odnosno prilikom analize rizika moguće je efikasno oceniti nivo zaštite za svaki pojedini resurs bitan za funkcionisanje poslovnih procesa unutar kompanije.

Kvalitetna identifikacija resursa doprinosi postizanju sledećih zahteva: identifikacija odgovornih lica, identifikacija pojedinih resursa bitnih za funkcionisanje poslovnih procesa, procena vrednost resursa, pronalaženje njihovog fizičkog ili logičkog

mesta u sistemu, formiranje odgovarajuće dokumentacije.

7.5.3.4 Podela resursa

Podela resursa se može realizovati prema raznim pravilima. U informacionim sistemima resurse je moguće grubo podeliti na sledeće kategorije:

- podaci (baze podataka, dokumentacija, autorska dela itd.),
- softverska podrška (aplikacije, operativni sistemi, razvojni alati itd.),
- oprema (računarska oprema, mrežno-komunikaciona oprema, mediji za čuvanje podataka i ostala oprema neophodna za rad informacionog sistema),
- servisi (računarski i komunikacioni odnosno uopšteno servisi).

Za svaki od definisanih resursa treba napraviti procenu njegove relativne vrednosti unutar sistema bez obzira kojoj kategoriji pripada. Bezbednost informacionih sistema može biti ugrožena na više načina. Možemo ih podeliti prema izvoru:

- ljudi – namerne pretnje,
- ljudi – nenamerne pretnje,
- oprema i prirodne nepogode.

Iako mnogi smatraju da pretnje bezbednosti sistema najčešće dolaze spolja, istraživanja koja su obavili određeni autori [566] pokazuju sasvim suprotne činjenice. Najveći procenat problema bezbednosti uzrokuju ljudske greške, dok je drugi najveći uzrok kvar opreme. Nakon toga sledi zaposleni koji svoj položaj na poslu koriste za sticanje sopstvene koristi i zaposleni koji na ovakav način izražavaju svoje nezadovoljstvo prema instituciji ili nadređenoj osobi.

Kako bi sprečili mogućnost realizacije ovakvih neželjenih radnji koji ugrožavaju integritet i bezbednost sistema neophodno je uvođenje odgovarajućih mera. Neprekidna edukacija zaposlenih, smeštanje opreme za čuvanje podataka u posebne prostorije, donošenje propisa kojima se određuje pristup, kontrolisanje atmosferskih uslova u takvoj prostoriji, utiče na duži radni vek opreme a time i pouzdaniji rad kompletnog sistema. Implementacijom kontrole pristupa podacima i definisanjem sankcija onima koji se ne pridržavaju propisanih pravila suzbija se zloupotreba sistema od strane zaposlenih. [566]

Napadi „spolja" donose najviše štete sistemu. Oni učestvuju u veoma malom procentu, a cilj im je pribavljanje informacija, njihovo menjanje ili uništavanje. Sistem se od takvih napada brani kontrolom saobraćaja sa Interneta prema sistemu i obrnuto, sprečavanjem instaliranja programa u operativni sistem ili kriptovanjem podataka.

7.5.3.5 Bezbednosne mere za zaposlene

Najveće pretnje informacionom sistemu su lica koji sa njim imaju vezu, kroz svakodnevni rad ili kroz povremeno održavanje. Analizirajući statistiku pretnji bezbednosnim sistemima, može se zaključiti da većina pretnji sistemima dolazi od lica koja dolaze u dodir sa njim, bez obzira na mo[illegible]. Kako računar omogućava i upade van kompanije, bezbednosne mere za zaposlene moraju obuhvatiti i lica koja ne rade u kompaniji ali sa njom dolaze u kontakt.

Svaka kompanija se mora osloniti na kvalitetne bezbednosne mehanizme za svoj personal. Praćenjem situacije u kompaniji i u okruženju, moguće je pravovremeno sprečiti potencijalne opasnosti i unaprediti bezbednosne mere. Operaciona bezbednost uključuje

dva aspekta bezbednosti informacionih sistema. Prvi se odnosi na povećanje svesti između potencijalnih žrtvi, a drugi predstavlja načine na koji se računarski kriminalci mogu sprečiti u izvršavanju dela. Povećanje svesti o važnosti bezbednosti može se postići uključivanjem zaposlenih u program bezbednosti. Potrebno ih je edukovati na koji način je bezbednost ugrožena i kako svi u kompaniji dele rizik i odgovornost. Jednom kada se analiziraju rizici sistema, potrebno je odrediti količinu informacija koja će se podeliti sa zaposlenima.

8. Kriptografija

Od jednostavnih početaka kriptografija je evolucijom postala složena matematička disciplinu koja obezbeđuje bezbednosne usluge poverljivosti, privatnosti, integriteta i provere identiteta. U ovom poglavlju rada na relativno jednostavan način biće predstavljeni osnovni kriptografski pojmovi, algoritmi i protokoli.

8.1 Osnovni kriptografski pojmovi

Kriptografija (engl. *cryptography*) je naučna oblast koja se bavi proučavanjem metoda za razmenu poruka u formi koja je čitljiva onima kojima je informacija namenjena dok je za ostale biti neupotrebljiva. [567][568] Izraz kriptografija izvedena je iz grčkog jezika od prideva kriptos (grč. *κρυπτός*) što znači „sakriven" i glagola grafo (grč. *γράφω*) što znači „pisati".[569] Definicije koje se mogu pronaći u literaturi zasnovane su na nameni kriptografije i ističu da ona predstavlja istraživanje matematičkih metoda vezanih za aspekte bezbednosti informacije kao što su: poverljivost (engl. *confidentiality*), integritet (engl. *integrity*), utvrđivanje identiteta (engl. *authentication*) i neporečivost (engl. *non-repudiation*). [570]

Kriptologija (engl. *cryptology*) predstavlja naučnu disciplinu – oblast koja se bavi istraživanjem i proučavanjem postupaka zaštite tajnosti informacija. Sačinjavaju ju je kriptografija i kriptoanaliza. [571] Uporedo sa razvojem kriptografije razvila se i kriptoanaliza koja za cilj ima da analizom šifrovane poruke otkrije njen sadržaj. [572]

Kriptoanaliza se bavi otkrivanjem šifri, odnosno otkrivanjem sadržaja otvorenog teksta na osnovu šifrata, pri čemu kriptografski ključ nije poznat. [573]

Izraz **kripto** u terminologiji obuhvata kriptologiju, kriptografiju, kriptoanalizu i razne druge teme iz oblasti zaštite. [573]

Originalna poruka (engl. *plaintext*) je polazna, čitljiva poruka koju na bezbedan način treba preneti do odredišta – otvoren tekst. [574]

Šifrovanje (engl. *encryption*) je proces maskiranja poruke sa ciljem skrivanja njene sadržine. [574]

Dešifrovanje (engl. *decryption*) je inverzivni postupak u kome se šifrovani podaci primenom ključa pretvaraju u originalnu poruku ili datoteku. [574]

Ključ (engl. *key*) se koristi za šifrovanje i dešifrovanje i služi za konfiguraciju šifarskog sistema kako bi on znao kako i na koji način da zaštiti određene podatke. [575]

Šifra (engl. *cipher*) je proces pretvaranja tajne poruke preslikavanjem u nerazumljiv niz znakova (slova, brojeva...), tako da je inverzna transformacija (dešifrovanje) jednoznačna. [576]

Kodom (engl. *code*) se jedna reč zamenjuje drugom reči ili simbolom. [577]

Kriptografski algoritam (engl. *cryptographic algorithm*) predstavlja matematičku funkciju koja se upotrebljava za šifrovanje i dešifrovanje. Ukoliko je bezbednost algoritma zasnovana na tajnosti načina rada algoritma, onda se radi o ograničenom (engl. *restricted*) algoritmu. [578]

Šifarski sistem (engl. *cryptosystem*) predstavlja matematičku funkciju koja se koristi za šifrovanje i dešifrovanje (algoritam sa svim mogućim otvorenim tekstovima, šifratima i ključevima). Šifarski sistemi se mogu podeliti na klasične i savremene.[579]

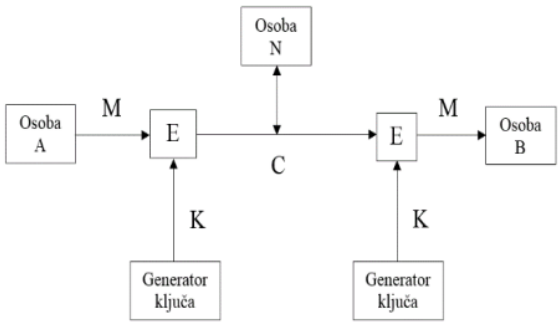
8.2 Šifarski sistemi

Pre ulaska računara u široku upotrebu, kriptografske metode šifrovanja zasnivale su se na tajnosti šifre. Ipak, tako zasnovani algoritmi pokazali su se kao veoma nepouzdani, što je zahtevalo pronalazak novih metoda šifrovanja. Današnje metode šifrovanja zasnivaju se na upotrebi ključa. Zavisno od načina korišćenja ključa, razvile su se dve vrste šifrarskih sistema. Postoje simetrični i asimetrični šifrarski sistemi. Osnovna razlika između ove dve vrste sistema je da simetrični šifarski sistem koristi isti ključ za šifrovanje i za dešifrovanje neke poruke, dok asimetrični šifrarski sistem koristi različite ključeve za šifrovanje i dešifrovanje poruke. Postoji i treća grupa šifrarskih sistema koji čine kombinaciju prethodna dva i oni se nazivaju hibridni.

8.2.1 Simetrični šifarski sistemi

Simetrični šifrarski sitemi (engl. *symetric algorithm*) su najčešći sistemi u kriptografiji. Kod ove vrste šifrarskih sistema ključ za šifrovanje i dešifrovanje isti je, po čemu su i dobili ime. Ključ za šifrovanje može biti izveden iz ključa za dešifrovanje, i obrnuto. [524] Kriptološka vrednost zasniva se na kvalitetu algoritma i na kvalitetu i tajnosti ključa, zbog čega ih nazivaju i šifarski sistemi tajnih ključeva. Ovi sistemi realizuju dve operacije, substituciju i transpoziciju. Odlikuju se velikom brzinom rada i jednostavnom implementacijom na računaru.

Osnovna karakteristika simetričnih šifarskih sistema (engl. *Symetric-Key* ili engl. *Secret-key Criptosystems*) je da se šifrovanje/dešifrovanje poruka vrši istim ključem. Blokovski prikaz simetričnog šifarskog sistema dat je na slici 64. Sa slike vidimo, da osoba A šalje poruku M osobi B putem nezaštićenog komunikacionog kanala. Ona najpre generiše poruku M i upućuje je u blok za šifrovanje E. Blok E vrši kriptovanje poruke M uz korišćenje ključa K dobijenog uz pomoć generatora ključa. Na taj način se kreira šifrovana poruka C. Potom se tako dobijena poruka komunikacionim kanalom šalje do osobe B. [578][580]



Slika 64. *Blokovski prikaz simetričnog šifarskog sistema*
Izvor: [573]

Postupak dešifrovanja vrši se inverznim postupkom u bloku za dešifrovanje D. Dešifrovanje poruke C se obavlja pomoću istog ključa K koji je korišćen prilikom šifrovanja. Nakon dešifrovanja se dobija izvorna poruka M. Ako na kanalu za komunikaciju postoji osoba N (napadač) koja može da presretne poslatu šifrovanu poruku i ukoliko dođe u posed ključa za dešifrovanje može pročitati ili zloupotrebiti izvornu poruku. [580]

Simetrično šifrovanje ima i određene nedostatke. Jedan od problema je taj da oba korisnika moraju imati isti simetrični ključ, pa se tada javlja problem distribucije odnosno međusobne razmene tih ključeva. Neophodno je da pošiljalac i primalac budu saglasni oko potrebe ključa pre nego što započnu sa bezbednosnom komunikacijom. Najpouzdaniji način je da se oba korisnika fizički sretnu i izvrše razmenu ključeva. Obzirom da su korisnici u najčešćem broju slučajeva fizički razdvojeni i njihov neposredan kontakt je nemoguć, za bezbednu razmenu ključeva se upotrebljava neki zaštićen kanal. Čest je slučaj i da kuriri lično prenose ključeve na odredišta. Ako je ključ otkriven (ukraden, pogođen, iznuđen, dobijen nelegalno...), nepoželjna osoba može da dešifruje sve poruke koje su šifrovane tim ključem. Nepoželjna osoba takođe može da se pretvara i da kao jedan od učesnika proizvodi lažne poruke kako bi izigrala drugu stranu. Dodatni problem simetričnih šifarskih sistema koji se može javiti je veliki broj potrebnih ključeva. Pod pretpostavkom da svaki par korisnika u mreži upotrebljava poseban ključ, ukupni broj ključeva brzo se uvećava kako raste broj korisnika.

Neki simetrični algoritmi su objavljeni (u celini ili delimično) i izloženi ozbiljnom, dugotrajnom ispitivanju. Drugi, tajnošću izbegavaju javnu ocenu svoje bezbednosti. Kod nekih od poznatih pronađene su statističke anomalije ili slabosti ključeva, neki su razbijeni i napušteni, a neki se unapređuju i dalje primenjuju. Simetrični algoritmi se dele u dve kategorije. U prvoj grupi se radi na otvorenom tekstu bit po bit (nekada i bajt po bajt) i oni se nazivaju sekvencijalni algoritmi (engl. *stream algorithms*), ili sekvencijalne šifre (engl. *stream cipher*). Rad na otvorenom tekstu u grupama bitova karakterističan je za drugu grupu. Grupe bitova se nazivaju blokovi (engl. *blocks*) a grupa se naziva blokovski algoritmi (engl. *block algorithms*) ili blokovske šifre (engl. *block ciphers*). [580]

Najpoznatiji algoritmi simetričnih šifarskih sistema koji su danas u upotrebi su: DES, 3DES, IDEA, Blowfish, AES, RC5, RC6 i drugi.

8.2.1.1 DES algoritam

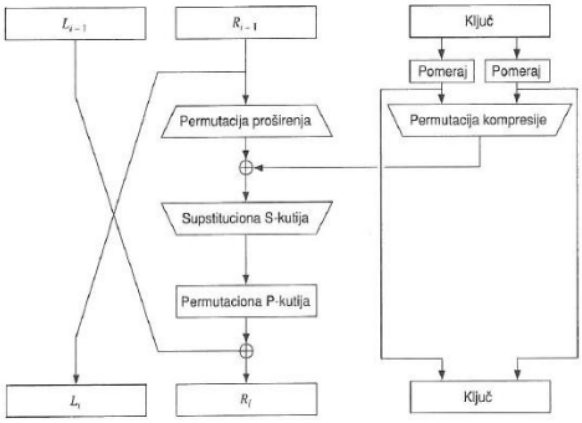
DES algoritam (engl. *Data Encryption Standard, DES*) pripada grupi blokovskih algoritama koji šifruju tekst u blokovima dužine 64 bita, koristeći ključ dužine 56 bita. Na taj način se dobija šifrat dužine 64 bita. Simetrični je algoritam (isti algoritam i isti ključ koriste se za šifrovanje i za dešifrovanje). [581] Dizajn algoritma utemeljen je na Lucifer šifri i Fejstel šifri koje je razvio tim IBM. [573] Fejstel šifra koju predstavlja DES ima sledeće parametre:

- dužina bloka otvorenog teksta je 64 bita;
- dužine ključa je 56 bitova sa ukupno 2^{56} mogućih ključeva;
- sastoji se od 16 rundi pre generisanja jednog bloka šifrata;
- dužina podključa koji se koristi u svakoj rundi je 48 bitova.

Algoritam DES radi na 64-bitnim blokovima otvorenog teksta. Nakon početne permutacije, vrši se podela bloka na desnu i levu polovinu, dužine po 32 bita. Nakon toga izvršava se 16 rundi identičnih operacija koje se nazivaju funkcija f, i u kojima se obavlja

kombinovanje podataka sa ključem. Posle 16 rundi leva i desna polovina se spajaju, dok završna permutacija koja je inverzna početnoj završava algoritam.

U svakoj rundi, bitovi ključa se pomeraju, a zatim se bira 48 bitova od 56 bitova ključa. Desna polovina podataka preko permutacije širenjem se proširuje do 48 bitova, kombinuje sa 48 bitova pomerenog i permutovanog ključa pomoću *XOR* operacije, ide kroz 8 S-kutija, gde se na kraju dodaje novih 32 bitova i ponovo se vrši permutacija. Ove četiri operacije predstavljaju funkciju f . Izlaz funkcije se potom kombinuje sa levom polovinom uz pomoć dodatne *XOR* operacije. Rezultat ovih operacija postaje nova desna polovina, a stara desna polovina postaje nova leva polovina. Ove operacije se ponavljaju 16 puta.



Slika 65. *Prikaz jedne runde DES algoritma*
Izvor: [582]

Ako je B_i rezultat $i-$te iteracije, L_i i R_i, su leva i desna polovina od B_i, K_i je 48-bitni ključ za rundu i, dok f predstavlja funkciju koja obavlja sve operacije supstitucije, permutacije i XOR operacije sa ključem.

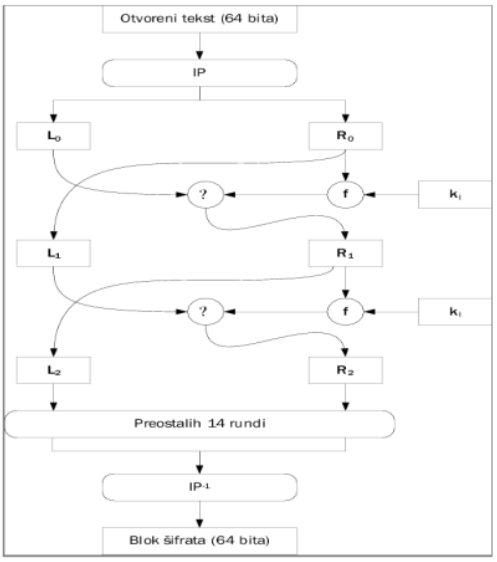
Osnovni koraci u DES algoritmu su: inicijalna permutacija IP, 16 rundi obrade podataka (proširenje, XOR sa ključem, supstitucija) i završna inverzna permutacija IP^{-1}.

Pomoću fiksne inicijalne permutacije IP i datog bloka otvorenog teksta x, dobija se vrednost $x_0 = IP(x)$ koja se može zapisati u obliku $x_0 = L_0R_0$, gde su $L_0 - 32$ viša bita u x_0 i $R_0 - 32$ niža bita u x_0.

Nakon početne permutacije, sledi 16 iteracija tj. rundi DES algoritma, koje su zasnovane na Feistelovoj mreži. Izlazni podatak $L_{i-1}R_{i-1}(1 \le i \le 16)$ iz prethodne runde (ulazni podatak za prvu rundu je vrednost dobijena inicijalnom permutacijom bloka otvorenog teksta), transformiše se 16 puta na sledeći način:

- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus f(R_{i-1}, ki)$

Simbolom $\oplus$ označena je operacija XOR, a $k_1, k_2, \ldots, k_{16}$ su potključevi, tj. ključevi runde dužine 48 bita dobijeni permutacijom nekih bitova iz ključa k. Na kraju se izlazni podatak poslednje runde pomoću završne permutacije IP^{-1} transformiše u šifrat dužine 56 bitova.

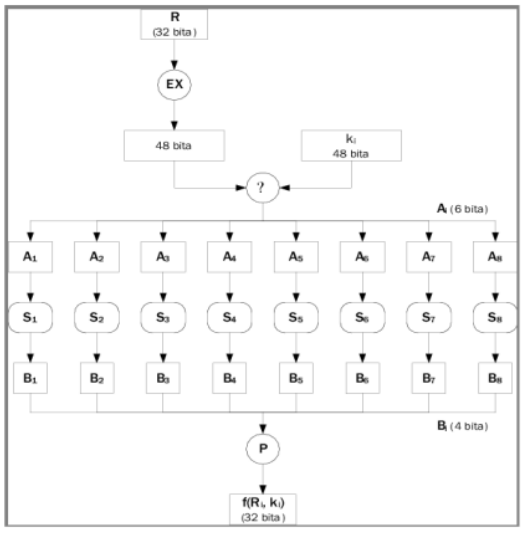


Slika 66. *Algoritam DES šema*
Izvor: [573]

Funkcija f zahteva dva ulazna argumenta: niža 32 bita izlaza iz prethodne runde (R_{i-1}) i potključ dužine 48 bitova (k_i). Za rezultat se dobija niz dužine 32 bita. Funkcija se izračunava u sledeća četiri koraka:

1. Niz R_{i-1} se proširuje do dužine 48 bitova prema fiksnoj funkciji proširenja EX. Rezultujući niz $EX(R_{i-1})$ sadrži 32 bita niza R_{i-1} permutovanih na određeni način, tako da se 16 bitova pojavljuje dvaput.
2. Zatim se izračunava vrednost $A = EX(R_{i-1}) \oplus k_i$ a rezultat zapisuje u obliku osam 6-bitnih nizova: $A = A_1A_2A_3A_4A_5A_6A_7A_8$.
3. Sledeći korak je zamena vrednosti A pomoću supstitucijskih kutija (engl. *supstitution box, S-box*). Svaka ova kutija $S_j(S_1S_2, \dots, S_8)$ predstavlja matricu fiksnih dimenzija 4×16, čiji su elementi celi brojevi između 0 i 15. Za dati niz od 6 bitova, $A_j = a_1a_2a_3a_4a_5a_6$, rezultat supstitucije $S_j(A_j)$ određuje se na sledeći način:
   - Dva bita a_1a_6 određuju binarni zapis reda $(0 \leq red \leq 3)$, a četiri bita $a_2a_3a_4a_5$ određuju binarni zapis kolone $(0 \leq kol \leq 15)$ u S_j.
   - $B_j = S_j(A_j) = S_j(red, kol)$, zapisano kao binarni broj dužine 4 bita.

   Na ovaj način se određuje $B = B_1B_2 \dots B_8 = S_1(A_1)S_2(A_2) \dots S_8(A_8)$.
4. Niz bitova B dužine 32 bita permutuje se pomoću fiksne završne permutacije P. Tako se dobija $P(B)$, tj. $f(R_{i-1})$.



Slika 67. *Funkcija f DES algoritma*
Izvor: [540]

Potključevi $k_1, k_2, \ldots, k_{16}$ se formiraju pomoću sledećeg postupka. Ključ k dužine 56 bitova upotrebljen prilikom šifrovanja, čuva se u obliku K u dužini od 64 bita. Bitovi parnosti na pozicijama 8, 16, 24, 32, 40, 48, 56 i 64 definisani su tako da svaki bajt sadrži neparan broj jedinica. Ovi bitovi se ignorišu pri izračunanju tabele ključeva.

Za 64-bitni ključ k, ignorišu se bitovi parnosti dok se preostalih 56 bitova permutuje pomoću fiksne permutacije PK_1. Zapisuje se $PK_1(k) = C_0D_0$, gde su C_0 i D_0 viši i niži 28 bitova u $PK_1(k)$. Za $I = 1,2, \ldots, 16$ računa se:

[1] $C_i = L_{Si}(C_{i-1})$,

[2] $D_i = L_{Si}(D_{i-1})$,

[3] $k_i = PK_2(C_iD_i)$.

LS_i predstavlja ciklični pomeraj ulevo za jednu poziciju, ako je $i = 1,2,9$ ili 16, a u ostalim slučajevima za dve pozicije. Pk_2 predstavlja fiksnu permutaciju.

Dešifrovanje DES šifrata postiže se primenom istog algoritma kao i za šifrovanje. Polazi se od šifrata y, ali se sada potključevi primenjuju u obrnutom redosledu: $k_{16} = k_{15} = \cdots = k_1$. Kao rezultat se dobija otvoreni tekst x.

Neki DES ključevi su značajno nebezbedni od ostalih, pa se i ne koriste. U te ključeve spadaju:

- Ključevi koji generišu jednake potključeve u svakoj rundi: $k_1 = k_2 = \cdots k_{16}$. Postupci šifrovanja i dešifrovanja slabim ključem su jednaki. Primer slabih DES ključeva su:
  - 0101010101010101
  - $1F1F1F1F0E0E0E0E$
  - $E0E0E0E0F1F1F1F1$
  - $FEFEFEFEFEFEFEFE$
- Parcijalno slabi ključevi, odnosno ključevi koji kreiraju samo dva različita

potključa, od kojih se svaki koristi u po 8 rundi. Par ključeva (k, k') su delimično slabi DES ključevi ako rezultat kompozicije dva DES algoritma sa ključevima k i k' predstavlja otvoren tekst. Jednostavnije rečeno, šifrovanje s jednim ključem isto je što i dešifrovanje s drugim. Postoji šest pari polovično-slabih DES ključeva:

- $01FE01FE01FE01FE$ i $FE01FE01FE01FE01$
- $1FE01FE00EF10EF1$ i $E0F1E0F1F10EF10E$
- $01E001E001F101F1$ i $E001E001F101F101$
- $1FFE1FFE0EFE0EFE$ i $FE1FFE1FFE0EFE0E$
- $011F011F010E010E$ i $1F011F010E010E01$
- $E0FEE0FEF1FEF1FE$ i $FEE0FEE0FEF1FEF1$

- Potencijalno slabi ključevi, odnosno ključevi koji kreiraju samo četiri potključa (48 ključeva). Ukupno ima 64 ključa koje ne treba koristiti.

Kriterijumi projektovanja i bezbednost DES algoritma – inicijalna i završna permutacija, ne utiču u velikoj meri na sigurnost algoritma, ali omogućavaju lakše učitavanje otvorenog teksta i šifrata bajt po bajt u hardversku implementaciju algoritma zasnovanu na 8-bitnom mikroprocesoru. Iz tog razloga neki proizvođači softvera preskaču IP i IP^{-1} i otvoren tekst direktno uvoze u prvu rundu.

Može se pokazati da je kriptoanaliza linearnih kriptosistema napadom, relativno jednostavna (na primer, napad na Hilovu šifru). Sve operacije u okviru DES algoritma, izuzimajući zamenu vrednosti u supstitucijskim kutijama su linearne što ukazuje na važnost S-kutija za bezbednost čitavog DES-a. One su projektovane tako da povećaju difuziju kriptosistema (na svaki bit šifrata utiče što više bitova otvorenog teksta) i otežaju diferencijalnu kriptoanalizu. Projektovanje S-kutija je obavila NSA prema sledećim kriterijumima:

- Svaki red S-kutije predstavlja permutaciju brojeva od 0 do 15.
- S-kutije su nelinearne i neafine funkcije ulaznih podataka.
- Promenom jednog bita ulaznog podatka prilikom primene S-kutija rezultuje u promeni najmanje 2 bita u izlaznom podatku.
- Za svaku S-kutiju i svaki ulazni podatak x važi da se vrednosti $S_j(x)$ i $S_j(x \oplus 001100)$ razlikuju u barem 2 bita.
- Za svaku S-kutiju, svaki ulazni podatak x i svako $e, f \in \{0,1\}$ važi sledeće: $S(x) \neq S(x \oplus 11ef00)$.
- Za svaku S-kutiju važi sledeće: ako se fiksira jedan bit u ulaznom podatku i posmatraju vrednosti jednog fiksnog izlaznog podatka, onda će broj ulaznih podataka kod kojih je taj bit jednak 0 biti blizu broja onih kod kojih je taj bit jednak 1. Preciznije, ako fiksiramo prvi ili šesti bit ulaznog podatka, onda su oba broja jednaka 16, dok kod drugih bitova variraju između 13 i 19.

Permutacije P su usklađene sa sledećim kriterijumima:

- Četiri izlazna bita svake S-kutije su ulazni podaci u sledećoj rundi za šest različitih S-kutija, dok nijedna dva nisu ulazni podaci za istu S-kutiju.

- Četiri izlazna bita svake S-kutije u i-toj rundi se distribuiraju tako da dva od njih utiču na središnje bitove u $i + 1$ rundi, a dva na krajnje bitove (dva leva i dva desna od 6 bitova u ulaznom podatku).
- Za dve S-kutije S_j i S_k važi sledeće: ako neki izlazni bit iz S_j utiče na neki središnji bit S_k u sledećoj rundi, onda nijedan izlazni bit iz S_k ne utiče na središnje bitove S_j.
- Za $j = k$: izlazni bitovi iz S_j ne utiču na središnje bitove S_j.

Standardi FIPS PUB 81 definiše četiri režima rada: ECB, CBC, OFB i CFB.[583] Standardi koji se koriste u bankama ANSI definišu ECB i CBC za šifrovanje, a CBC i $n-$bitni CFB za proveru identiteta.[584] Kada je u pitanju softverska implementacija, sertifikacija obično nije predstavljala problem, jer se zbog svoje jednostavnosti ECB se najčešće koristi u gotovim komercijalnim proizvodima, iako je samo najranjiviji pri napadima. Režim CBC se povremeno koristi, jer je malo komplikovaniji od režima ECB, a pruža mnogo veću bezbednost. [585][586][587][588]

Promene jednog bita otvorenog teksta ili jednog bita ključa treba da utiču na više bitova šifrata. Ako je promena u šifratu mala, značajno se smanjuje broj otvorenih tekstova ili ključeva koji treba da budu ispitani prilikom kriptoanalize. Osobina da se malom promenom otvorenog teksta ili ključa značajno menja šifrat karakteristično je za DES i u literaturi se može naći pod imenom „efekat lavine" (engl. *avalanche*).

Pokazuje se da efekat lavine dolazi do izražaja već u trećoj rundi, dok posle pete runde svaki bit šifrata zavisi od svakog bita otvorenog teksta i ključa. Takođe, uočava se da je posle osme runde šifrat slučajna funkcija bitova otvorenog teksta i ključa. Posle 16 rundi poznati napadi (na primer, diferencijalna kriptoanaliza) ne mogu da budu efikasniji od napada grubom silom. [589]

Verzija algoritma koja je Američkom nacionalnom birou za standarde ponuđena od strane IBM-ovih kriptografa koristila je ključ dužine 112 bitova. U verziji koja je prihvaćena kao standard, dužina ključa je pod uticajem biroa smanjena na 56 bitova. DES, sa ključem dužine 56 bitova, danas ne pruža dovoljnu bezbednost protiv napada grubom silom.

Diffie i Hellman su 1977. godine [590] utvrdili da se pomoću tadašnje tehnologije može konstruisati računar koji bi otkrio ključ za jedan dan. Obzirom visoke troškove otkrivanja ključa koji tada procenjeni na 20 miliona dolara zaključeno je da je takav računar dostupan samo vojnim organizacijama i organizacijama kao što je NSA, ali da će 1990. godine DES algoritam postati sasvim nebezbedan. Campbell i Weiner su 1993. godine tvrdili da se za 100.000 dolara može napraviti računar koji bi otkrio ključ za 35 časova, za milion dolara računar koji bi otkrio ključ za 3,5 časa, dok se za 10 miliona dolara dobija računar koji otkriva ključ za 21 minut. [591] Konačno razbijanje DES-a usledilo je 1998. godine od strane organizacije *Electronic Frontier Foundation (EFF)* sa softverom *DES Cracker* koji košta 250.000 dolara, a otkriva ključ za 56 časova. Sagrađen je od 1.536 čipova koji mogu ispitati 88 milijardi ključeva u sekundi.

Eli Biham i Adi Shamir [592] su javno 1993. godine demonstrirali metodu diferencijalne kriptoanalize. Osnovna ideja se sastoji u poređenju rezultata operacije XOR, koja je izvršena nad dva otvorena teksta sa rezultatom iste operacije izvršene nad dva odgovarajuća šifrata. Prosto rečeno, posmatra se blok od dva otvorenog teksta sa specifičnim razlikama i analizira se evolucija te razlike pri prolasku kroz algoritam. Različitim ključevima se dodeljuju verovatnoće na osnovu razlika u dobijeni šifratima.

Potom se ispituje veći broj parova otvorenog teksta i tako određuje najverovatniji ključ. Metoda je očigledno bila poznata konstruktorima DES, što se vidi iz načina na koji su konstruisane supstitucijske kutije i permutacija P.

Mitsuru Matsui, japanski kriptograf je 1993. godine predložio metodu linearne kriptoanalize. Pomoću ove metode, najverovatnije nepoznate tvorcima DES-a, zasniva se aproksimacija linearnom funkcijom nekih bitova ključa iako oni nisu linearne funkcije otvorenog teksta i šifrata. Pomoću nje je Matsui opisao napad tipa poznati otvoreni tekst koji za razbijanje DES-a zahteva prosečno 2^{43} otvorenih tekstova. Ni linearna ni diferencijalna kriptoanaliza nisu dovele do razbijanja DES-a, ali je njihova važnost u tome što su primenljive na svaki simetričan blokovski algoritam. [593]

8.2.1.2 AES

Algoritam AES (engl. *Advanced Encryption Standard*, *AES*) predstavlja jedan od algoritama za zaštitu podataka. Zasniva se na simetričnom Rijandael algoritmu, a kao standard razvijen je da bi se postepeneo zamenio DES, čija bezbednost u današnjim uslovima više nije dovoljna. Kao algoritam AES je definisan i prihvaćen od strane NIST (engl. *National Institute of Standards and Technology*, *NIST*) u 197 dokumentu FIPS-a, 2. januara 1997. godine, pa se kao takav može primenjivati u državnim i drugim institucijama SAD. Za AES su odabrani algoritmi sa dužinom ključa 128, 192 i 256 bita, dok je dužina bloka za sve tri dužine ključa 128 bita.

Algoritam AES razlikuje se od svojih prethodnika u kriptografiji kao prvi algoritam koga karakteriše brzina izvršavanja i u softverkoj i u hardverskoj implementaciji. Zbog veoma malog utroška memorije, AES algoritam je pogodan za izvršavanje i na skromnijim ugrađenim sistemima. Bazira se na principu permutacije i supsitucija. Izvršava se nad 4x4 matricom bajtova, koja se zove stanje, koju čini blok od 128 bita ulaznog teksta. Dužina ključa pri šifrovanju ili dešifrovanju određuje broj ponavljanja transformacija (kombinacija permutacija i supstitucija) nad ulaznim nizom zvanim tekst, i konačnim izlazom, zvanim šifrovan tekst. Broj transformacija je sledeći:

- 10 za ključ dužine 128 bita
- 12 za ključ dužine 192 bita
- 14 za ključ dužine 256 bita

Svaki drugi krug sastoji se od nekoliko koraka, od kojih svaki sadrži 4 slične operacije, uključujući jednu koja zavisi od samog ključa. Set obrnutih rundi primenjuje se za dešifrovanje podataka. Ovaj algoritam pokazao se kao veoma pouzdan u industriji, i predviđa se da će ostati dominantan kriptografski alat i u sledećih 50 godina.

Algoritam AES ima sledeće funkcionalne parametre:

- dužina bloka otvorenog teksta je 128, 192 i 256 bitova,
- dužina ključa je 128, 192 i 256 bitova,
- broj rundi je promenjiv, i zavisi od dužine ključa i veličine bloka,

Mnogi simetrični blokovski algoritmi zasnovani su na primeni Feistelovih mreža – blok podataka se razdvaja na dva dela koji pri prenosu u narednu rundu menjaju mesta, s tim da se nad jednim blokom obavi izvesni funkcija: $L_i = R_{i-1}, R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$. Kod RIJNDAEL algoritma postoje runde koje se razlikuju od Feistelovih. Jedna RIJNDAEL runda sadrži tri nivoa:

- linearni difuzioni sloj (engl. *linear mixing layer*) - obezbeđuje veliku difuziju bitova nakon nekoliko rundi (funkcije *ShiftRow* i *MixColumn*),
- nelinearni sloj (engl. *non-linear layer*) – primenjuju se supstitucijske kutije optimizovanih za najgori slučaj (funkcija *ByteSub*),
- sloj dodavanja ključa (engl. *key addition layer*) – obavljaju se XOR operacije nad potključem runde sa trenutnim stanjem bloka (funkcija *AddRoundKey*).

Prethodno navedeni slojevi projektovani su pomoću specijalnih metoda, sa posebnim osvrtom na otpornost protiv diferencijalne i linearne kriptoanalize (*Wide Tail Strategy, WTS*).

Matematičke osnove za AES algoritam zasnivaju se na sledećim pokazateljima. Svaki oktet RIJNDAEL algoritma interpretira se kao element konačnog polja $GF(2^8)$ (engl. *Galois field*). Oktet se prikazuje kao niz bitova $b_7, b_6 \dots b_0$ ili kao element konačnog polja, primenom sledeće notacije: [582]

- $b_7X^7 + b_6X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X^1 + b_0X^0 = \sum_i b_i\, X^i.$

Na primer, oktet 0110 1011 (69h) može se prikazati kao element konačnog polja: $X^6 + X^5 + X^3 + 1$. Elementi u konačnom polju sabiraju se pomoću operacije XOR primenjene nad odgovarajućim bitovima polinoma. Na primer,

- $(X^7 + X^6 + X^5 + 1) + (X^6 + X^5 + X + 1) = (X^7 + X)$

Množenje u konačnom polju GF (28) istovetno je množenju polinoma po modulu $m(X)$, gde je $m(X)$ nedeljiv polinom osmog stepena. Primenom operacije deljenja po modulu obezbeđuje se da će rezultat biti stepena manjeg od 8, tj. da se rezultat može prikazati kao polinom. Množenje je asocijativno, a multiplikativna konstanta je 1. Operacije množenja i sabiranja su distributivne. RIJNDAEL kao nedeljivi polinom koristi $m(X) = (X^8 + X^4 + X^3 + X + 1)$ Na primer,

- $(X^6 + X^4 + X^2 + X + 1) \cdot (X^7 + X + 1) mod\ (X^8 + X^4 + X^3 + X + 1) = (X^7 + X^6 + 1)$

Za svaki polinom $b(X)$ koji je različit od nula polinoma može se definisati inverzni polinom $b^{-1}(X)$. Pomoću proširenog Euklidovog algoritma izračunavaju se polinomi $a(X)$ i $c(X)$ takvi da je: $b(X) \cdot a(X) + m(X) \cdot c(X) = 1$. Zato je: $a(X) \cdot b(X)\ mod\ m(X) = 1$, što znači $b^{-1}(X) = a(X)\ mod\ m(X)$.

RIJNDAEL primenjuje i operacije nad polinomima sa koeficijentima iz $GF\ 2^8$ stepena manjeg od 4. Koeficijenti, kao i elementi konačnog polja, tj. okteti, a ne bitovi ukazuju na razliku pomenutik polinoma i polinoma koeficijenata stepena $GF\ 2^8$. Svaki polinom oblika $a(X) = a_3X^3 + a_2X^2 + a_1X + a_0$ se predstavlja kao četvorobajtni vektor tj. kao 32-bitna reč $a_0a_1a_2a_3$. Sabiranje takvih polinoma je sabiranje (tj. na izvođenje operacije XOR) koeficijenata članova istog stepena. U cilju dobijanja polinoma stepena manjeg od četiri, množenje se obavlja po modulu polinoma četvrtog stepena (za to je izabran polinom $X^4 + 1$). Rezultat množenja polinoma $a(X)$ i $b(X)$ po modulu $X^4 + 1$, jeste polinom četvrtog stepena d(X) definisan na sledeći način:

- $d(X) = d_3X^3 + d_2X^2 + d_1X + d_0$, gde su:
- $d_0 = (a_0 \cdot b_0) \oplus (a_3 \cdot b_1) \oplus (a_2 \cdot b_2) \oplus (a_1 \cdot b_3)$
- $d_1 = (a_1 \cdot b_0) \oplus (a_0 \cdot b_1) \oplus (a_0 \cdot b_2) \oplus (a_3 \cdot b_3)$
- $d_2 = (a_2 \cdot b_0) \oplus (a_1 \cdot b_1) \oplus (a_0 \cdot b_2) \oplus (a_3 \cdot b_3)$

- $d_3 = (a_3 \cdot b_0) \oplus (a_2 \cdot b_1) \oplus (a_1 \cdot b_2) \oplus (a_0 \cdot b_3)$

Pri tome se koeficijenti a_i i b_i množe kao polinomi po modulu $m(X)$.

Šifrovan – Stanje bloka (engl. *state*) ukazuje na trenutno stanje šifrovanog bloka podataka. Ono se može zamisliti kao matrica bajtova promenljive veličine (blok za šifrovanje je promenljive veličine), pa se ova matrica naziva matrica stanja. Za blok podataka veličine 192 bita matrica stanja će biti dimezija 6x4 (tabela 27).

Tabela 27. *Matrica stanja za 192-bitni blok*
Izvor: [540]

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$	$S_{0,4}$	$S_{0,5}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,4}$	$S_{1,5}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$	$S_{2,4}$	$S_{2,5}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$	$S_{3,4}$	$S_{3,5}$

Pomoću svake ćelije predstavlja se jedan bajt, tj. oktet. U matricu se upisuju ulazni okteti redom po kolonama. Broj redova matrice je fiksan, odakle zaključujemo da svaka kolona ima ukupno 32 bita, tj. 4 okteta. Broj kolona matrice N_w je zavistan od veličine bloka za šifrovanje i dobija se podelom veličine bloka sa 32. Matrica stanja algoritma AES uvek je veličine 4x4 okteta, dok originalni algoritam RIJNDAEL dopušta i druge vrednosti.

Ključ za šifrovanje se predstavlja pomoću tabele sa četiri reda i N_k kolona, slično stanju bloka. Primera radi, za 192-bitni ključ, tabela ključa će imati oblik (tabela 28):

Tabela 28. *Tabela ključa AES algoritma*
Izvor: [540]

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$	$k_{0,4}$	$k_{0,5}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$	$k_{1,4}$	$k_{1,5}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$	$k_{2,4}$	$k_{2,5}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$	$k_{3,4}$	$k_{3,5}$

Ovako predstavljeno stanje i ključ olakšavaju logičku analizu algoritma i koriste se interno u algoritmu.

Broj rundi u algoritmu (N_r) je promenljiv, i u direktnoj je korelaciji sa veličinom bloka i dužinom ključa. Konkretno, broj rundi je određen onim što je duže - $\max(N_w, N_k)$. Ako su i ključ i blok dužine 128 bitova $N_w = N_k = 4$, onda je broj rundi 10. Ukoliko su ili ključ ili blok podatka dužine 192 bita $N_w = 6$ ili $N_k = 6$, onda je broj rundi 12. Ako su ili ključ ili blok podatka dužine 256 bitova $N_w = 8$ ili $N_k = 8$, onda je broj rundi 14. Što se tiče AES standarda, blok je uvek dužine 128 bitova, a ključevi mogu biti dužine 128 bitova (AES-128), 192 bita (AES-192) i 256 bitova (AES-256).

U algoritmu RIJNDAEL operacije se izvode na matrici stanja. Kopiranjem ulaznog bloka podataka u matricu stanja započinje se proces šifrovanja. Nakon kopiranja, matrica stanja inicijalno dobija potključ (*AddRoundKey*). Zatim se ona u zavisnosti od dužine ključa, transformiše 10, 12 ili 14 puta, tako da se poslednja runda transformacija razlikuje od prethodnih (izostavlja se transformacija *MixColumn*. U svakoj rundi algoritma vrše se četiri transformacije nad oktetima:

- zamena okteta na osnovu tabele supstitucije (*ByteSub*)

Jedina nelinearna transformacija je funkcija *ByteSub*: najpre se vrši zamena elemenata matrice svojim multiplikativnim inverznim elementima u konačnom polju $GF(2^8)$ (element 00h ostaje nepromenjen), a zatim se primenjuje sledeća transformacija nad bitovima matrice stanja:

$$b'_i = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus b_{(i+7)mod8} \oplus c_i$$

b_i je $i-$ti bit okteta, a $c_i i-$ti bit okteta $c = 63h = 01100011$. Funkcija *ByteSub* se može prikazati pomoću supstitucione kutije. Red u supstitucionoj kutiji određen je sa četiri viša bita okteta, dok je kolona predstavljena sa četiri niža bita okteta. Na primer, oktet 69h se transformiše pomoću funkcije *ByteSub* u $F9h$.

- pomeranje okteta u redovima matrice stanja (*ShiftRow*)

Funkcija *ShiftRow* vrši rotaciju okteta u redovima matrice stanja za jedno (drugi red), dva (treći red) i tri mesta ulevo (četvrti red), tako da se prvi red matrice $(r = 0)$ ne pomera.

- $s_{0,0}s_{0,1}s_{0,2}s_{0,3} \rightarrow s_{0,0}s_{0,1}s_{0,2}s_{0,3}$
- $s_{1,0}s_{1,1}s_{1,2}s_{1,3} \rightarrow s_{1,1}s_{1,2}s_{1,3}s_{1,0}$
- $s_{2,0}s_{2,1}s_{2,2}s_{2,3} \rightarrow s_{2,2}s_{2,3}s_{2,0}s_{2,1}$
- $s_{3,0}s_{3,1}s_{3,2}s_{3,3} \rightarrow s_{3,3}s_{3,0}s_{3,1}s_{3,2}$
- mešanje podataka u kolonama matrice stanja (*MixColumn*)

Funkcijom *MixColumn* vrši se transformisanje u svakoj koloni matrice stanja. Kolone se posmatraju kao polinomi četvrtog stepena $s(X)$ sa koeficijentima iz $GF\ (2^8)$ i u tom obliku se množe sa konstantnim polinomom četvrtog stepena $a(X) = 03X^3 + 01X^3 + 01X + 02$ po modulu $m(X) = X^4 + 1$ Tj. $s'(X) = s(X) \cdot a(X)$. Izmenjena matrica stanja sastoji se od sledećih okteta:

- $s'[0,k] = (02 \cdot s[0,k]) \oplus (03 \cdot s[1,k]) \oplus s[2,k] \oplus s[3,k]$
- $s'[1,k] = s[0,k] \oplus (02 \cdot s[1,k]) \oplus (03 \cdot s[2,k]) \oplus s[3,k]$
- $s'[2,k] = s[0,k] \oplus s[1,k]) \oplus (02 \cdot s[2,k]) \oplus (03 \cdot s[3,k])$
- $s'[3,k] = (03 \cdot s[0,k] \oplus s[1,k]) \oplus s[2,k]) \oplus (02 \cdot s[3,k])$
- dodavanje potključa u matricu stanja (*AddRoundKey*)

Funkcija *AddRoundKey* vrši transformaciju matrice stanja dodavanjem potključa pomoću operacije XOR. Svaki potključ se sastoji se od N_w reči iz linearnog niza dobijenog proširenjem ključa. Te reči se dodaju na sledeći način:

$$[s'[0,k], s'[1,k], s'[2,k], s'[3,k]] = [s[0,k], s[1,k], s[2,k], s[3,k]] \oplus [W_{runda} * N_{w+k}], \text{za } 0 \leq k < N_w$$

- W_i su reči niza dobijenog proširenjem ključa, promenljiva runda dobija vrednost tekuće runde algoritma $0 \leq runda \leq N_r$.

Završna vrednost matrice stanja kopira se u izlazni šifrovani blok podataka.

Proširenje ključa – Obavlja se kako bi se generisali odgovarajući potključevi za operaciju *AddRoundKey*. Proširenjem ključa stvara se $(N_r + 1)N_w$ 32-bitnih reči, koje su označene sa $W_i(0 \leq i < (N_r + 1)N_w)$. Biraju se iz proširenog ključa tako da se prvi međuključ sastoji od prve četiri reči, drugi od sledeće četiri.

Početne četiri reči proširenog ključa predstavlja ključ k. Svaka sledeća reč se dobija primenom operacije XOR nad prethodnom reči i reči koja se nalazi N_k pozicija pre tekuće $(W_i = W_{i-1} \oplus W_i - N_k)$. Ako je i deljivo sa N_k, onda se pre operacije ekskluzivno ILI nad reči W_{i-1} izvršavaju operacije:

- *RotWord*, koja rotira reč W_{i-1} jedno mesto ulevo, tako da se od reči $b_0b_1b_2b_3$

dobije reč $b_1 b_2 b_3 b_0$,

- *SubWord*, koja na reč W_{i-1} primenjuje supstitucionu kutiju i
- XOR reči W_{i-1} sa konstantom runde (konstanta $rconst[i]$ runde i ima vrednost $[02^{i-1}, 00, 00, 00]$.

Dešifrovanje se vrši primenom istog algoritma, ali se u rundama koriste funkcije inverzne funkcijama *ByteSub*, *ShiftRow* i *MixColumn*, i nepromenjena funkcija *AddRoundKey*.

Ako se algoritam za šifrovanje predstavi sledećim pseudokodom:

```
stanje=ulaz;
AddRoundKey(stanje,w[0,Nw-1]);
for runda=1 to Nr-1 do {
   ByteSub(stanje);
   ShiftRow(stanje);
   MixColumn(stanje);
   AddRoundKey(stanje,w[runda*Nw,(runda+1)*Nw-1]);
}
ByteSub(stanje);
ShiftRow(stanje);
AddRoundKey(stanje,w[Nr*Nw,(Nr+1)*Nw-1];
izlaz=stanje;
```

algoritam za dešifrovanje imaće sledeći oblik:

```
stanje=ulaz;
AddRoundKey(stanje,w[Nr*Nw,Nr+1)*Nw-1]);
for runda=Nr-1 to 1 do {
   ShiftRowInv(stanje);
   ByteSubInv(stanje);
   AddRoundKey(stanje,w[runda*Nw,(runda+1)*Nw-1]);
   MixColumnInv(stanje);
}
ShiftRowInv(stanje);
ByteSubInv(stanje);
AddRoundKey(stanje,w[0,Nw-1]);
```

Funkcija *ByteSubInv* predstavlja inverznu funkciju funkciji *ByteSub*. Na primer, ulazni oktet $F9h$ ova funkcija transformiše u $69h$. Oktet $00h$ ostaje nepromenjen. Funkcija *ShiftRowInv* vrši rotaciju okteta u redovima matrice stanja za jedno (drugi red), dva (treći red) i tri mesta udesno (četvrti red), s tim što se prvi red matrice ($r = 0$) ne pomera. Pomoću funkcije *MixColumnInv* vrše se transformacije u svakoj koloni matrice stanja – kolone se predstave kao polinomi četvrtog stepena $s(X)$ sa koeficijentima iz $GF(2^8)$ i množe sa konstantnim polinomom četvrtog stepena $a^{-1}(X) = 0B9x^3 + 0Dx^2 + 09x + 0E$ po modulu $m(X) = X^4 + 1$. Tj. $s'(X) = s(X) \cdot a^{-1}(X)$. Polinom $a^{-1}(X)$ je multiplikativni inverzni element polinoma $a(x)$ koji koristi funkcija *MixColumn*. Izmenjena matrica stanja sastoji se od sledećih okteta:

- $s'[0,k] = (0E \cdot s[0,k]) \oplus (0B \cdot s[1,k]) \oplus (0D \cdot s[2,k]) \oplus (09 \cdot s[3,k])$
- $s'[1,k] = (09 \cdot s[0,k]) \oplus (0E \cdot s[1,k]) \oplus (0B \cdot s[2,k]) \oplus (0D \cdot s[3,k])$
- $s'[2,k] = (0D \cdot s[0,k]) \oplus (09 \cdot s[1,k]) \oplus (0E \cdot s[2,k]) \oplus (0B \cdot s[3,k])$
- $s'[3,k] = (0B \cdot s[0,k]) \oplus (0D \cdot s[1,k]) \oplus (09 \cdot s[2,k]) \oplus (0E \cdot s[3,k])$

Bezbednost AES algoritma – U ovom trenutku dužine ključeva za definisane

standarde AES-128, AES-192 i AES-256 su dovoljne za bezbednosne zahteve u većini primena. U algoritmu do sada nisu pronađeni nebezbedni ili potencijalno nebezbedni ključevi. Otpornost algoritma RIJNDAEL na linearnu i diferencijalnu kriptoanalizu ukazuje da je prilikom razvoja algoritma posebna pažnja bila posvećena tome da sve moguće strategije napada imaju očekivano trajanje i memorijske zahteve identične onima pri napadima na ostale algoritme koji šifruju blokove podataka iste dužine, ili veće od tih zahteva.

Obzirom da AES nije osetljiv na napade korišćenjem linearne i diferencijalne kriptoanalize, neke naznake ukazuju da je osetljiv na algebarske napade, a posebno na novu XSL (engl. *eXtended Sparse Linearization, XLS*) metodu napada. Neki primeri su pokazali da se takvim napadom postižu mnogo bolji rezultati nego napadima primenom sile (engl. *brute force attack*). U ovom trenutku izvođenje takvih napada još uvek nije praktično moguće, međutim, oni pokazuju da i ovaj standard ima svoje određene nedostatke.

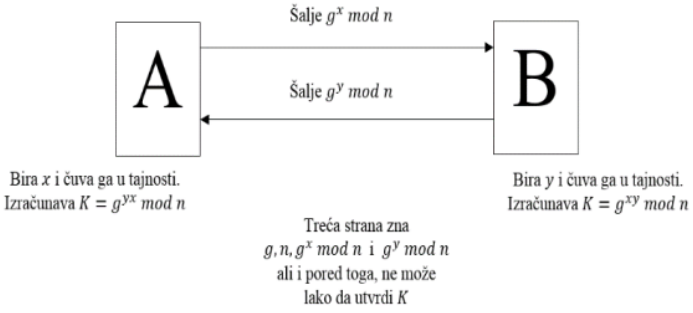
Ostaje da se vidi da li će biti pronađene slabosti i nedostaci ovog algoritma. Jedan od osnovnih postulata kriptografije i kriptoanalize jeste da nema apsolutno bezbednog algoritma, već je samo pitanje vremena i sredstava potrebnih da dođe do probijanja. Očekivano je da će se u budućnosti ipak predstaviti neki drugi standard koji bi trebalo da ispuni sve zahteve moderne kriptografije.

8.2.2 Diffie-Hellman protokol za razmenu ključeva

Prvu kriptografsku šemu za razmenu javnih ključeva predstavlja Diffie-Hellman protokol. Predložen je od strane Witfielda Diffija i Martina Hellmana 1976. godine. [594] On omogućava razmenu tajnih ključeva, bez prethodno dogovaranih tajni. Britanska tajna služba *GCHQ* (engl. *Government Communications Headquarters, GCHQ*) je već pre 1976. godine razvila takav protokol, ali ga je držala u tajnosti. Možda je i pre toga već bio otkriven, s obzirom na jednostavnost, ali svakako nije bio objavljivan. Protokol nosi ime po svojim kreatorima: Whitfield Diffie i Martin Hellman. Danas postoji više implementacija ovog protokola, tako da originalno nije predviđen za implementaciju pomoću eliptičkih krivulja, ali je ime još ostalo povezano uz osnovnu ideju. IEEE je predložila standard sa ovim protokolom kao osnovnim algoritmom za razmenu ključeva, ali postoje i još neke poboljšane ideje koje rešavaju neke probleme. Ovaj algoritam bio je patentiran, ali je istekao i nije objavljen.

Protokol koristi dva ključa (jedan tajni i jedan javni). Prilikom procesa komunikacije, pošiljalac šifruje poruku sa svojim tajnim ključem i javnim ključem primaoca. Primalac vrši dešifrovanje poslate poruku korišćenjem svog tajnog ključa i javnog ključa pošiljaoca. Težina Diffie-Hellman protokola je u izračunljivosti logaritamske funkcije za eksponente koji su prosti brojevi tj. problemu diskretnog logoritma u konačnom polju. Sam algoritam se može koristiti za distribuciju ključeva (Alisa i Bob mogu da koriste ovaj algoritam kako bi generisali tajni ključ), ali se algoritam ne može koristiti za šifrovanje i dešifrovanje poruka.

Razmena ključeva u Diffie-Hellman protokolu funkcioniše tako što pošiljaoc i primaoc razmene izračunate vrednosti na osnovu kojih se može utvrditi vrednost ključa za šifrovanje.



Slika 68. *Difie-Hellman razmena ključeva*
Izvor: [595]

U izračunavanjima se mogu koristiti brojevi koji ne moraju da budu tajni. Na primer, dve strane mogu da se slože oko korišćenja dva cela broja g i n za izračunavanje ključa za šifrovanje. Na slici 68 prikazana je razmena između strana A i B i ilustrovano je ko šta zna.

Prvo A vrši izbor celog broja x i izračunava i šalje vrednost $g^x \ mod \ n$ do B. Na sličan način, B nezavisno bira vrednost y i do A šalje vrednost izraza $g^y mod \ n$. Ukoliko treća strana prisluškuje njihovu komunikaciju, pretpostavimo da zna vrednosti g i n, zajedno sa onim što se prenosi. U međuvremenu do A stiže vrednost $g^y mod \ n$ koji tu vrednost stepenuje na x, tako da se dobije $g^{yx} \ mod \ n$. Nasuprot tome, B prima $g^x \ mod \ n$ i stepenuje tu vrednost na y, i dobija $g^{xy} \ mod \ n$. Na osnovu karakteristika modularne aritmetike, $g^{yx} \ mod \ n$ je isto što i $g^{xy} \ mod \ n$ odakle zaključujemo da A i B koriste isti ključ za šifrovanje.

Kao što smo već napomenuli, treća strana zna vrednosti g i n i može da utvrdi vrednost $g^x \ mod \ n$ i $g^y \ mod \ n$ osluškujući komunikacionu liniju. Obzirom da A i B kriju vrednosti x i y, treća strana ne može da kompletira izračunavanja potrebna za utvrđivanje ključa za šifrovanje. Primetimo da ovo ne garantuje sigurnost komunikacione linije. Nameće se logično pitanje, da li treća strana može na osnovu informacija koje ima da zaključi koje su vrednosti za x i y? Ona mora da izračuna vrednost logaritma $g^x \ mod \ n$ ili $g^y \ mod \ n$. Postoje uslovi koje g i n moraju da zadovoljavaju kako bi takva izvođenja bila veoma teška. g i n moraju da budu veoma veliki brojevi (možda od po hiljadu bitova).

Diffie-Hellman protokol razmene ključeva je osetljiv na problem koji je poznat kao man-in-the-middle napad. Pretpostavimo da u komunikaciji postoji i treća strana – E. Osoba E povezuje se na liniju kojom komuniciraju A i B. Sa jedne strane ulovi javni ključ od A, a sa druge strane javni ključ od B. Zatim i A i B pošalje svoj javni ključ. I A i B ne znaju da komuniciraju preko E. Tako da sada E dešifruje podatke koje šalje A, čita ih, ponovo ih šifruje i prosleđuje B. Takođe, E je u mogućnosti da izmeni podatke.

Matematički to izgleda ovako. Kod ovog napada „uljez" se postavlja između A i B. Kada A pošalje $g^x \ mod \ n$, „uljez" vrši presretanje te vrednosti i njeno menjanje sa vrednošću $g^{x'} \ mod$, koju prosleđuje do B. Ni A ni B toga nisu svesni. Kada B pošalje $g^y \ mod \ n$, „uljez" ponovo presreće tu vrednost, menja je u $g^{y'} \ mod \ n$ i šalje do A čega ponov ni A ni B nisu svesni.

Zatim, osoba A vrši šifrovanje pomoću ključa $g^{xy'} \ mod \ n$ koji koristi i „uljez". Slično tome, B koristi ključ $g^{x'y} \ mod \ n$ koji „uljez" takođe, koristi za komuniciranje sa B. A i B misle da direktno komuniciraju, a zapravo „uljez" presreće sve njihove poruke,

dešifruje ih i ponovo ih šifruje, pre nego što ih prosledi do druge strane. [596]

Jedan od načina izbegavanja ovakvog napada je komuniciranje putem više linija, kojima napadač nema pristup. Bolji protokol od ovde navedenog je Menezes-Qu-Vanstone (MQV) koji Diffie-Hellmanov protokol i onemogućava *man-in-the-middle* napad tako što traži autentifikaciju.

Generisanje simetričnog ključa kada je u pitanju Diffie-Hellman protokol odvija se na istom kanalu kao i glavna komunikacija. Snaga ovog protokola je korišćenje diskretnog algoritma koji se može smatrati neizračunivim za dovoljno velike parametre. Loša strana je ta što je neophodno da se koriste velike vrednosti koje troše resurse i samu operaciju čine skupom. Pored toga, jer kao takav protokol pruža visoku tajnost, pre započinjanja protokola učesnici su obavezni da se identifikuju, pa je samim tim neophodna jednostrana autentifikacija. Obično je ta strana servis. [597]

Diffie-Hellman protokol nije ograničen samo na dva učesnika A i B, već se može razmatrati bilo koji broj učesnika. Ovaj protokol se koristi kao deo infrastrukture javnih ključeva mada je danas RSA algoritam dominantan. Ne koristi se za potpisivanje sertifikata, za koji se koriste ElGamal i RSA.

8.2.3 Asimetrični šifarski sistemi

Algoritmi sa javnim ključem (engl. *pubik-key algorithms*) poznati kao asimetrični algoritmi (engl. *asymmetric algorithms*) pronađeni su u sedamdesetim godinama 20. veka. Kod njih se za šifrovanje i dešifrovanje koriste različiti ključevi. Njihovi tvorci, Whitefield Diffie i Martin Hellman su 1976. godine opisali ideju kriptografije koja se zasniva na dva ključa, privatnom (i često zvanim tajnim) i javnom ključu. Ideja je bila u primeni funkcija za šifrovanje e_K iz kojih je praktično nemoguće, u nekom razumnom vremenskom roku, izračunati funkciju za dešifrovanje d_K.

U svrhu realizacije ovakvih šifarskih sistema, koriste se osobine jednosmerne funkcije. Za funkciju $f: X \to Y$ kažemo da je jednosmerna funkcija (engl. *one-way function*), ako je $f(x)$ lako izračunati za svaki $x \in X$, dok je $f^{-1}(y)$ izračunavanje jako teško. Ako se f^{-1} može lako izračunati ukoliko nam je poznat neki dodatni podatak (engl. *trapdoor* – tajni ulaz), onda za funkciju f kažemo da je samostalna jednosmerna funkcija (engl. *trapdoor one-way function*).

Algoritam sa javnim ključem sastoji se od dva skupa funkcija. Funkcije za šifrovanje e_K i funkcija za dešifrovanje d_K, gde K prolazi skupom svih mogućih korisnika, sa svojstvom:

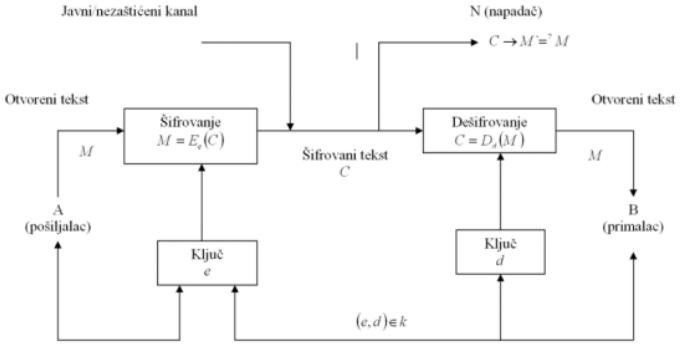
1. Za svaki K d_K je inverzno od e_K.
2. Za svaki K e_K je javan, ali je d_K poznat samo osobi K.
3. Za svaki K e_K je samostalna jednosmerna funkcija.

Ključ e_K se naziva javni ključ, a d_K se naziva tajni (privatni) ključ.

Ključevi su međusobno povezani složenim transformacijama takve prirode da obezbeđuju da se bez poznavanja specijalne, tajne informacije, jedan ključ praktično ne može dobiti iz drugog. [524]

Oba ključa su povezana pomoću jedinstvene jednosmerne funkcije sa zamkom, tj. ne sme doći do izračunavanja tajnog ključa iz javnog ključa ili se barem ne sme izračunati

u razumnom vremenskom roku. Osim toga, ključ za dešifrovanje ne sme (bar ne u razumnom vremenskom roku) biti izveden, tj. biti izračunat iz ključa za šifrovanje. Šifrovanje je jednostavan smer. Instrukcije za šifrovanje su javni ključ: svako može da šifruje poruku. Dešifrovanje je težak smer jer je otežano dovoljno da oni koji trenutno imaju najsavremenije računare na svetu ne bi mogli za desetine godina da dešifruju poruku ako ne znaju zamku (tajnu) – privatni ključ (slika 69). [598]



Slika 69. *Ilustracija postupka asimetričnog šifrovanja*
Izvor: [598]

Radi jednostavnije analize rada upotrebljavaćemo simbole A, B i N. Simbolom A je označena osoba koja želi da pošalje izvorni tekst, dok B ukazuje na osobu koja bi trebala da primi poslati tekst, a N na osobu koja neovlašćeno želi da dođe do sigurnih podataka koje osobe A i B razmenjuju. Asimetrično šifrovanje se odvija po sledećem scenariju: Osoba A vrši šifrovanje poruke radi njenog slanja osobi B pomoću javnog ključa osobe B koji je svima dostupan (čak i osobi N). Osoba A može da dobije taj javni ključ putem e-mail-a, preuzeti sa web sajta i sl. Ipak, i pored toga što se poznaje javni ključ ne može doći do otkrivanja sadržaja poruke. Dešifrovanje poruke može izvršiti samo osoba B korišćenjem svog tajnog ključa. Na ovaj način poruka postaje zaštićena od trećeg lica. Nedostatak ovog načina šifrovanja je njegova sporost i neprikladnost za šifrovanje velikih količina podataka. Ipak, ostaje otvoreno pitanje autentičnosti poruke.

U uslovima elektronskih komunikacija sa velikim brojem učesnika, funkcionisanje kriptozaštite ovakvim sistemima zadržava poznate i otvara nove probleme. Najveći problemi su: distribucija ključeva šifrovanja i utvrđivanje verodostojnosti poruke. Dobre osobine asimetrične kriptografije su: distribucija ključeva i upravljanje ključevima. Najčešće se primenjuju sledeći asimetrični algoritmi: RSA (*Rivest-Shamir-Adleman*), Diffie-Hellman, ElGamal, Eliptic Curves, Rabin i drugi.

8.2.3.1 RSA algoritam

Nakon Merkleovog algoritma za problem ranca, pojavio se prvi kompletan algoritam s javnim ključem RSA algoritam, koji funkcioniše i za šifrovanje i za digitalne potpise. [599][600] Od svih algoritama koji primenjiuju javne ključeve, RSA je najjednostavnije razumeti i realizovati. Martin Gardner je objavio opis ovog algoritma. [601] Algoritam je nazvan prema trojici autora američkih naučnika Ronald Linn Rivest, Adi Shamir i Leonard Adleman, čija početna slova prezimena i određuju skraćenicu RSA. Mora se napomenuti da je RSA algoritam izdržao godine opsežne kriptoanalize. Obzirom da kriptoanaliza nije ni dokazala, niti dovela u pitanje bezbednost RSA algoritma, ona ukazuje na nivo poverenja koji zaslužuje ovaj algoritam.

Bezbednost algoritma zasniva se na problemu faktorizacije (pronalaženja prostih činilaca) velikih brojeva. Iako je nalaženje velikih prostih brojeva (većih od 100 do 200 cifrenih ili većih) računarski lako, faktorizacija proizvoda dva takva broja je računski praktično nerešiva. S druge strane, provera da li su određeni brojevi faktori (činioci) velikog broja je jednostavna i brza, pa je ovaj problem pogodna osnova za ugradnju jednosmerne funkcije i mogućnost ugradnje tajnog grananja. Rekonstrukcija otvorenog teksta na osnovu javnog ključa i šifrata smatra se ekvivalentnim faktorisanjem proizvoda ta dva prosta broja.

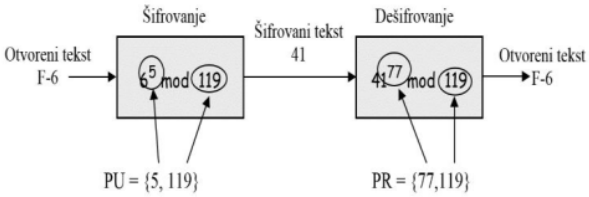
Algoritam RSA funkcioniše na sledeći način. Za kreiranje javnog i tajnog ključa se koriste veliki prosti brojevi. Tajni ključ predstavlja uređeni par brojeva (n,d). Javni ključ predstavlja uređeni par brojeva (e,n). Treba primetiti da je broj n zajednički za oba ključa. Osoba koja šalje poruku vrši kriptovanje pomoću formule:

$$C = M^e \bmod n$$

gde je: M izvorni tekst koji je prikazan u obliku broja, C broj koji predstavlja šifrovan tekst a brojevi e i n su komponente javnog ključa. Nakon prijema poruke vrši se njeno dešifrovanje pomoću sledeće formule:

$$M = C^d \bmod n = \left(M^e\right)^d \bmod n = M^{ed} \bmod n$$

gde su M i C iste vrednosti kao i u prethodnoj formuli, a n i d predstavljaju komponente tajnog ključa. Primer RSA šifrovanja prikazan je na slici 70.



Slika 70. *Ilustracija RSA šifrovanja*
Izvor [602]

U primeru sa slike 70, tajni ključ predstavlja uređeni par (119, 77), a javni ključ je uređeni par (119,5). Predpostavimo da osoba A želi da pošalje karakter F osobi B. Karakter F se može predstaviti kao broj 6 (F je šesti karakter u abecedi). Primenom formule algoritma šifrovanja dobija se $C = 6^5 \bmod 119 = 41$ koji se šalje kao šifrovan tekst osobi B. Kada primi broj, osoba B koristi algoritam za dešifrovanje i dobija vrednost $P = 41^{77} \bmod 119 = 6$, koja se inverznom transformacijom vraća u karakter F.

Ovde se sada postavlja pitanje pouzdanosti ovakvog načina razmene poruka. Ako neka treća osoba C zna formulu za dešifrovanje i $N = 119$, a nedostaje joj samo $d = 77$, ona može da izvrši nasumično "pogađanje" broja d. U prethodno datom primeru osoba C bi mogla da i pogodi vrednost d, ali je osnovni koncept RSA za d i e takav da predviđa korišćenje veoma velikih brojeva. To u praksi znači da se veliki broj kombinacija moraju isprobati radi otkrivanja šifre tj. veoma je dugo vreme razbijanja koda čak i uz pomoć najbržih računara koji su danas dostupni. [603]

Osnovni problem je kako izabrati brojeve n, d i e (veoma velike vrednosti dužine od 1.024 do 2.048) a da ujedno zadovoljavaju formule algoritma.

8.2.3.1.1 Definicija RSA šifarskog sistema

Bezbednost RSA algoritma je u činjenici da je faktorizacija velikih prirodnih brojeva na proizvod dva prosta broja teško izvodljiva. U skladu sa definicijom koja kaže da je šifarski sistem uređena petorka (P,C,K,E,D) za koju je [604][602][605][606]

- P – *konačan skup svih mogućih otvorenih tekstova.*
- C – *konačan skup svih mogućih šifrata.*
- K – *prostor ključeva, tj. konačan skup svih mogućih ključeva.*
- *za svaki ključ* $K \in K$ *postoji algoritam šifrovanja* $e_k \in E$ *i odgovarajući algoritam dešifrovanja* $d_k \in D$, *gde su* $e_k : P \to C$ *i* $d_k : C \to P$ *funkcije sa svojstvom da je*

$$d_k(e_k(x)) = x$$

za svaki otvoreni tekst $x \in P$.

RSA šifarski sistem se može i preciznije definisati.

Definicija 1. Neka je $n = p \cdot q$, gde su p i q prosti brojevi i neka je $P = C = Zn = \{0,1,2,\ldots, n-1\}$

kao i

$$K = \{(n,p,q,d,e) \div n = p \cdot q, de \equiv 1 (\mathrm{mod}\ \varphi(n))\}$$

gde je $\varphi(n) = (p-1)(q-1) = n - p - q + 1$ Ojlerova funkcija, koja prirodnom broju n pridružuje broj prirodnih brojeva manjih od n, koji su relativno prosti. Iz njenog svojstva da je $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$ za $nzd(a,n) = 1$ sledi da su funkcije e_K i d_K jedna drugoj inverzne.

Za $K = (n,p,q,d,e) \in K$ definišemo

$$e_K(x = x^e) \bmod n \qquad d_K(y) = y^d \bmod n$$

gde su $x, y \in Zn$.

Vrednosti n i e su javne, dok su vrednosti p,q i d tajne.

Sigurnost RSA šifarskog sistema je u pretpostavci da je funkcija:

$$e_K(x) = x^e \bmod n$$

jednosmerna.

Ovde je $x^e \bmod n$ jednosmerna funkcija, a *trapdoor* je poznavanje faktorizacije $n = pq$.

Poznavanjem faktorizacije broja n može se izračunati $\varphi(n) = (p-1)(q-1)$ a zatim dobiti eksponent d rešavajući linearnu kongruenciju

$$de \equiv 1 (\mathrm{mod}\ \varphi(n))$$

pomoću proširenog Euklidovog algoritma.

Ostaje nam još da proverimo jesu li funkcije e_K i d_K jedna drugoj inverzne. Pre toga iskažimo i dokažimo Ojlerovu teoremu.

Definicija 2. *Za neki prirodan broj n, skup od $\varphi(n)$ celih brojeva $\{a_1, a_2, ..., a\varphi(n)\}$ se zove* redukovani sistem ostataka *modulo n ako sadrži tačno po jedan element svake klase ostataka modulo n koji je relativno prost sa n.*

Teorema 1 [Ojler]. *Ako je $M(a,m)=1$, onda je* $a^{\varphi(m)} \equiv 1 \pmod m$.

Dokaz: Neka je $\{r_1, ..., r_{\varphi(m)}\}$ redukovani sistem ostataka modulo m.

Kako je $M(a,m)=1$, imamo da je $M(ar_i, m)=1$, za sve $i=1,...,\varphi(m)$. Nadalje, za svaki $i \in \{1,...,\varphi(m)\}$ postoji $\sigma(i) \in \{1,...,\varphi(m)\}$ takav da je

$$ar_i \equiv r_{\sigma(i)} \pmod m.$$

Šta više, $ar_i \equiv ar_j \pmod m$ ako i samo ako je $i=j$, pa je σ neka permutacija skupa $\{1,...,\varphi(m)\}$, a skup $\{ar_1, ..., ar_{\varphi(m)}\}$ je takođe redukovani sistem ostatka modulo m. Sada je:

$$a^{\varphi(n)} \cdot r_1 \cdot r_2 .. r_{\varphi(m)} \equiv (a \cdot r_1) \cdot (a \cdot r_2) .. (a \cdot r_{\varphi(m)}) \pmod m$$
$$\equiv r_{\alpha(1)} \cdot r_{\alpha(2)} ... r_{\alpha(n)} \pmod m$$
$$\equiv r\varphi(1) \cdot r\varphi(2) ... r\varphi(m) \pmod m$$

Podelimo li obe strane ove kongruencije sa $r_1 \cdot r_2 \cdot ... \cdot r_{\varphi(m)}$, što smemo jer su brojevi r_i relativno prosti sa m, dobijamo da je

$$a^{\varphi(m)} \equiv 1 \pmod m$$

Proverimo sada jesu li funkcije e_K i d_K jedna drugoj inverzne.

$$d_K(e_K(x)) \equiv (e_K(x))^d \equiv (x^e)^d \equiv x^{de}$$

Obzirom da je $de \equiv 1 (\mathrm{mod}\ \varphi(n)))$, to znači da postoji prirodan broj t takav da je $de = t \cdot \varphi(n) + 1$ pa imamo

$$x^{de} \equiv x^{t\varphi(n)+1} \equiv x^{t\varphi(n)} x \equiv (x^{\varphi(n)})^t x$$

U zavisnosti od n i x imamo 2 slučaja:

1. $M(x,n)=1$

Kako je tada, prema Ojlerovoj teoremi, $x^{\varphi(n)} \equiv 1 \pmod n$, onda je

$$x^{de} \equiv 1^t \cdot x \equiv x \pmod n.$$

2. $M(x,n) \neq 1$

Ako je $M(x,n)=n$, tada je $x=0$ pa je kongruencija trivijalno zadovoljena.

Neka je $M(x,n)=p$ ili $M(x,n)=q$. Bez smanjenja opštosti uzmimo da je

$M(x,n)=p$, pa je $x^{de}\equiv 0\equiv x(\mathrm{mod}\ p)$. Kako je $M(x,pq)=p$, gdje su p i q prosti, to je $M(x,q)=1$ pa je prema Ojlerovoj teoremi

$$x^{\varphi(q)}\equiv 1(\mathrm{mod}\ q)\Rightarrow x^{q-1}\equiv 1(\mathrm{mod}\ q).$$

Sada je

$$x^{de}=\left(x^{(q-1)}\right)^{(p-1)}\cdot x\equiv x(\mathrm{mod} q).$$

Konačno je $x^{de}\equiv x(\mathrm{mod}\ pq)$, tj. $x^{de}\equiv x(\mathrm{mod}\ n)$.

8.2.3.1.2 Implementacija RSA šifarskog sistema

RSA problem je težak pod predpostavkom da je modul n dovoljno veliki i slučajno izabran i kada je osnovna poruka M (a samim time i šifrovana poruka C) slučajno izabran ceo broj između 0 i n - *1*. Pretpostavka, u stvari kaže da je RSA funkcija *trapdoor* jednosmerna (pri čemu je privatni ključ *trapdoor*).

Sledi opis primene RSA algoritma.

1. Neka Bob tajno izabere dva različita prosta broja p i q, sa po 100 cifara. Oni se obično biraju tako da jedan od njih ima nekoliko cifara više od drugog. Pomoću nekog generatora slučajnih brojeva, generiše se dovoljno veliki prirodan broj k, a zatim se primenom nekog testa za testiranje prostosti, traži prvi prosti broj koji je veći ili jednak k.

2. Potom se izračunava $n=pq$ i $\varphi(n)=(p-1)(q-1)$.

3. Bira se na slučajan način broj e takav da je $e<\varphi(n)$ i $M(e,\varphi(n))=1$.

4. Izračunava se d takvo da je $de\equiv 1(\mathrm{mod}\ \varphi(n))$, tj. $d\equiv e^{-1}(\mathrm{mod}\ \varphi(n))$. Izračunavanje d se vrši pomoću *proširenog Euklidovog algoritma*, koji za date a i b računa $b^{-1}\ \mathrm{mod} a$.

Generisanje ključa	
Odrediti p,q	p i q oba prim, $p\neq q$
Izračunati $n=p\cdot q$	
Izračunati $\varphi(n)=(p-1)(q-1)$	
Odrediti ceo broj e	$(\varphi(n),e)=1;1<e<\varphi(n);M(e,\varphi(n))$
Izračunati d	$d\equiv e^{-1}(\mathrm{mod}\ \varphi(n))$
Javni ključ	$PU=\{e,n\}$
Tajni ključ	$PR=\{d,n\}$
Šifrovanje Boba sa Alis ključem	
Otvoreni tekst:	$M<n$
Šifrovani tekst:	$C=M^e \mathrm{mod} n$
Dešifrovanje Alis sa njenim javnim ključem	
Šifrovani tekst:	C
Otvoreni tekst:	$M=C^d \mathrm{mod} n$

Slika 71. *Ilustracija RSA šifrovanja (2)*
Izvor: [582]

Postupak šifrovanja poruke odnosno određivanja šifrata $y = x^e \bmod n$, naziva se modularno potenciranje. Za efikasnost RSA tajnarskog sistema bitno je da se računanje $x^e \bmod n$ može vrlo efikasno sprovesti pomoću algoritma „kvadriraj i množi":

$y = 1$

za $i = l-1,\ldots 1,0$ radi

$y = y^2 \bmod n$

ako je $e_i = 1$ tada je $y = y \cdot x \bmod n$

gdje je $e = \sum_{i=0}^{l-1} e_i 2^i$ binarni zapis broja e.

Primer 1. Predstavimo simulaciju da Alice šalje poruku OSIJEK NA DRAVI, Bobu i kako je on dešifruje.

Bob bira $p = 47$ i $q = 59$ i računa

$$n = p \cdot q = 2773$$
$$\varphi(n) = (p-1)(q-1) = 2668$$

Zatim bira $e = 17$ i pomoću proširenog Euklidovog algoritma izračunava d takvo da je $de \equiv 1 (\bmod \varphi(n))$ i dobija da je $d = 157$.

Vrednost p, q, d zadržava za sebe, a n i e šalje Alice.

Alice želi poslati poruku OSIJEK NA DRAVI, čiji je numerički ekvivalent

$$x = 15190910051100140100041801220,$$

jer je $(razmak = 00, A = 01, B = 02, \ldots, Y = 25, Z = 26)$.

Kako je $x > n$ to se x razbija u četvorocifrene blokove, sa početkom na levoj strani. Ukoliko zadnjem bloku nedostane cifara, on se dopunjuje nulama. Sada je:

$$x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = (1519,\ 0910,\ 0511,\ 0014,\ 0100,\ 0418,\ 0122,\ 0900).$$

Poznavajući Bobove javne $n = 273$ i $e = 17$, Alice računa

$$y_1 = 1519^{17} \bmod 2773 = 1204$$
$$y_1 = 910^{17} \bmod 2773 = 883$$
$$y_1 = 511^{17} \bmod 2773 = 680$$
$$y_1 = 14^{17} \bmod 2773 = 2049$$
$$y_1 = 100^{17} \bmod 2773 = 1952$$
$$y_1 = 418^{17} \bmod 2773 = 1983$$
$$y_1 = 122^{17} \bmod 2773 = 1384$$
$$y_1 = 900^{17} \bmod 2773 = 1510$$

Dobijeni šifrat

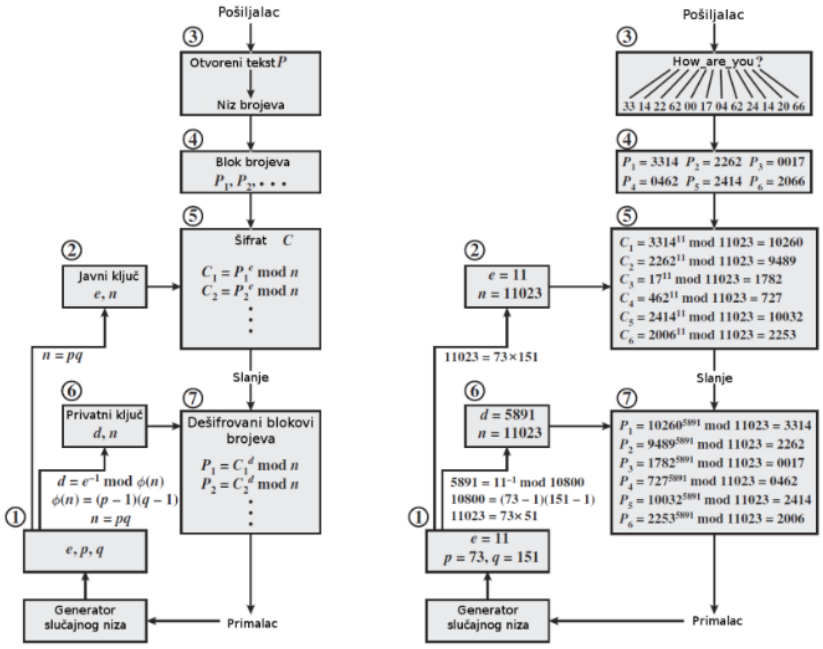
$$y = (yx_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8)$$
$$= (1204,\ 0883,\ 0680,\ 2049,\ 1952,\ 1983,\ 1384,\ 1510)$$
$$= 120408830680204919521983138415 10$$

šalje Bobu. Bob pomoću $d = 157$, koji je samo njemu poznat, računa, na isti način deleći y na blokove,

$$x_i = y_i^{157} \bmod 2773, i = 1,2,...,8$$

i dobija originalnu poruku OSIJEK NA DRAVI.

Dokaz prethodnih tvrdnji u primeru za RSA algoritam kao blok šifru predstavljen je na slici 72 kroz generalni pristup matematičkim operacijama u algoritmu i primeru praktične realizacije.



Slika 72. *Ilustracija matematičke i praktične realizacije RSA algoritma*
Izvor: [607]

8.2.3.1.3 Bezbednost RSA algoritma

Bezbednost RSA algoritma potpuno zavisi od faktorisanja velikih brojeva. Tehnički, to nije tačno. Pretpostavlja se da bezbednost RSA zavisi od problema sa faktorisanjem velikih brojeva. Nikada nije matematički dokazano da treba faktorisati n kako bi se izračunalo m iz c i e. Moguće je da će biti otkriven sasvim drugačiji način da se kriptoanalizira RSA. Međutim, ako taj novi način omogući kriptoanalitičaru da izvede d on bi mogao biti iskorišćen i kao nov način za faktorisanje velikih brojeva. Moguće je i da se RSA algoritam napadne pogađanjem vrednosti $(p-1)(q-1)$. Ovaj napad nije lakši od faktorisanja n.[608] Onima koji su posebno sumnjičavi, neke varijante RSA dokazano su teške kao što je faktorisanje.[609] Razlog za to je taj što se pokazuje da je otkrivanje samo nekih bitova informacije iz teksta šifrovanog algoritmom RSA podjednako teško kao dešifrovanje cele poruke.

Faktorisanje n je najočigledniji način napada. Svaki neprijatelj će imati javni ključ e i moduo n. Da bi pronašao ključ za dešifrovanje, d, on mora da faktoriše n. Do skoro je modul od 129 decimalnih cifara bio na granici tehnologije faktorisanja. Zato n mora da

bude veći broj od toga. Svakako je moguće da kriptoanalitičar isproba svaku mogućnost vrednosti d, sve dok ne naiđe na pravu. Ovaj napad grubom silom manje je efikasan čak i od pokušaja da se faktoriše n.

Tabela 29. *Jačina RSA ključa*
Izvor: [582]

Veličina Modula RSA (bit)	Bezbednost od faktorizacije (bit)
1024	86
1536	103
1792	110
2048	116
2560	128
3072	138
4096	156

S vremena na vreme, ljudi izjave kako su pronašli lak način da se probije RSA, ali se do danas nijedna takva izjava nije održala. Na primer, Vilijam Pejn je 1993. godine, u jednom nacrtu rada predložio metodu zasnovanu na maloj Fermaovoj teoremi.[610] Nažalost, ova metoda je takođe sporija od faktorisanja modula.

Tabela 30. *Preporuka minimalnog simetričnog nivoa i veličine RSA*
Izvor: [582]

period zaštite podataka	sadašnjica – 2010	sadašnjica – 2030	sadašnjica – 2031
Minimalni nivo simetrične bezbednosti	80 bita	112 bita	128 bita
Minimum veličine RSA ključa	1024 bita	2048 bita	3072 bita

Postoji još jedan razlog za brigu. Većina uobičajenih algoritama za izračunavanje prostih brojeva p i q probabilistički su: šta se dešava ako je p ili q složen? Prvo možete da učinite verovatnoću tog događaja proizvoljno malom. Ako se to ipak dogodi, tada šifrovanje i dešifrovanje verovatno neće raditi ispravno – što ćete svakako primetiti. Postoji nekoliko brojeva, pod nazivom Karmajklovi brojevi, koji neki probabilistički algoritmi za ispitivanje da li je broj prost neće otkriti. Oni su izuzetno retki.[611]

Tabela 31. *Preporuka minimalnog simetričnog nivoa i veličine RSA*
Izvor: [582]

Preporučeni period upotrebe	Preporučena namena
RSA 1024 ≤n≤2048	tokom 2010. prihvatljiv, zastareo u periodu 2011–2013, nakon 2013. neprihvatljiv
RSA n≥2048	prihvatljiv

Za ličnu upotrebu obično se koriste brojevi n od 1024-bita, odnosno $n \approx 10^{308}$. Za komercijalnu upotrebu preporučuju se brojevi n od 2048-bita, odnosno $n \approx 10^{617}$. Za važne potrebe koriste se brojevi od 4.096-bita odnosno $n \approx 10^{1234}$.

Teorijsko rešenje TWRL (engl. *The Weizmann Institute Relation Lokatora)* predstavlja novi hardverski dizajn za faktorizaciju brojeva, koji su razvili Shamir i Tromer. Kroz pristup faktorizacije brojeva utemeljenih na *Number Field Sieve*[612] dovelo je u pitanje sigurnost 1024 bitnih modula. NIST savetuje da je 80-bitni bezbednosni nivo (1024-bitni RSA ključ) bio dovoljan za zaštitu podataka do 2015. godine, dok će 112-bitni

sigurnosni nivo biti dovoljan do 2035. godine.[613] Napredovanjem tehnologije i brzine računara, vreme za faktorisanje se smanjuje, pa se u skladu sa tim povećava i broj n.[614]

8.2.3.1.4 Praktična iskustva u napadima na RSA algoritam

Očigledan napad na RSA algoritam je faktorizacija broja n. Napadač može pronaći $\varphi(n)$, a samim tim i d. Ipak, danas najbrži algoritmi za faktorisanje trebaju da imaju $e^{O\left((\log n)^{1/3}(\log\log n)^{2/3}\right)}$ operacije [615], tako da se smatraju relativno sigurnim ključevi od 2046 bita. Ipak, ovde još treba reći da iako još uvek nije poznat ni jedan polinomijalni algoritam za faktorizaciju, u nekim slučajevima n je p[29] lakše faktorizovati, pa takve n je potrebno izbegavati. Na primer, ako su p i q veoma blizu jedan drugog ili ako $p-1$ i $q-1$ imaju samo male proste faktore.

Ako napadač otkrije tajni eksponent d, promena eksponenta e nije dovoljna, već se mora menjati i n. [600][599] [29]

Treba izbeći generisanje različitih modela $n=pq$ i izabrati jedno kvalitetno n za sve korisnike, a da se iz jednog poverljivog centra korisnicima distribuiraju parovi e_K, d_k pomoću kojih bi oni formirali svoje javne (n, e_K) i tajne (n, d_K) ključeve. Ideja je loša, jer daje nesiguran sistem, pošto se pomoću e i d može faktorisati n. Dakle, bilo koji korisnik bi pomoću svog javnog i tajnog ključa mogao da faktoriše n, a zatim mu ne bi bilo teško da nađe privatni ključ bilo kog drugog korisnika. [29]

Na prvi pogled dobra ideja je i da se izabere malo d kako bi se smanjilo vreme potrebno za dešifrovanje. Međutim, teorema M. Wienera iz 1990. godine pokazuje da izbor malog d dovodi do lakog razbijanja šifre. [616] Boneh i Durfee su proširili Wienerov napad d[29]lučaja kada je $d \le n^{0,292}$. [617] Trebalo bi izbegavati slučaj kada je $d < \sqrt{n}$.

Postoje i napadi na RSA uz pretpostavku da je eksponent e mali, pa bi i to trebalo izbegavati. U ranijim implementacijama šifarskog sistema, često se uzimalo $e=3$, da bi se smanjilo vreme potrebno za šifrovanje. Međutim, takav izbor za e nije dobar. [618][619]

Džudit Mur izdvaja nekoliko ograničenja primene RSA algoritma, na osnovu uspešnosti navedenih napada. [620][621]

- Poznavanje jednog para eksponenata za šifrovanje/dešifrovanje za dati modul, omogućava napadaču da faktoriše taj modul.
- Poznavanje jednog para eksponenata za šifrovanje/dešifrovanje za dati modul, omogućava napadaču da izračuna druge parove za za šifrovanje/dešifrovanje, pri čemu mora da faktoriše n.
- Ne treba upotrebljavati zajednički modul u protokolu koji koristi RSA algoritam u komunikacionoj mreži.
- Poruke treba dopunjavati slučajnim vrednostima da bi se sprečili napadi na male eksponente za šifrovanje.
- Eksponent za dešifrovanje treba da bude veliki.

Takođe, potrebno je uvek imati na umu i da ovo sve nije dovoljno za bezbedan kriptografski algoritam. Ceo šifarski sistem mora da bude bezbedan, kao i kriptografski protokol. Propust u nekoj od ovih oblasti čine nebezbedan čitav sistem.

8.2.3.1.5 Standardi RSA

Sam RSA je *de facto* standard u velikom delu sveta. Organizacija ISO je skoro, ali ne sasvim, napravila RSA standard za digitalne potpise i u informacionom aneksu za ISA 9796. [622] Francusko udruženje banaka prihvatilo je RSA kao standard, [623] a tako su postupili i Australijanci. [624] Sjedinjene Američke Države trenutno nemaju nikakav standard za šifrovanje s javnim ključem, zbog pritiska iz Nacionalne agencije za bezbednost, NSA i patentnih zahteva. Mnoge američke kompanije koriste standarde PKCS, koji je napisan u kompaniji *RSA Data Secirity, Inc. – RSADSI*. U nacrtu ANSI standarda za bankarsko poslovanje navodi se RSA. [625]

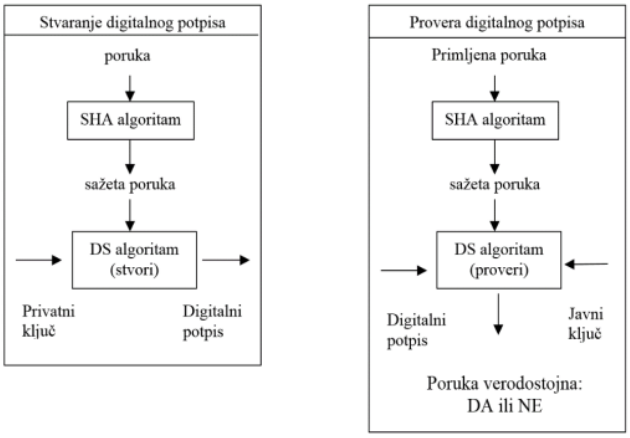
Algoritam RSA patentiran je u SAD [626], ali nije patentiran ni u jednoj drugoj zemlji. Kompanija *Public Key Partners – PKP* licencira taj patent, zajedno sa drugim kriptografskim patentima s javnim ključem. Američki patent istekao je 20. septembra 2000. godine.

8.2.3.2 Digitalni potpis

Digitalni potpis (engl. *Digital Signature*) predstavlja metod za identifikaciju potpisnika elektronskih poruka i dokumenata. Njegova namena je da potvrdi autentičnost sadržaja poruke, i obezbedi garantovanje identiteta pošiljaoca poruke. Pored toga što obezbeđuje autentičnost, digitalni potpis obezbeđuje i integritet, kao i neporečivost.

Osnova digitalnog potpisa je sadrž poruke. Pošiljalac primenom kriptografskih algoritama od svoje poruke najpre generiše zapis fiksne dužine (npr. 512 ili 1024 bita) koji u potpunosti odslikava sadržaj poruke. U procesu generisanja digitalnog potpisa za dobijanje sažete verzije poruke (engl. *message digest*) koristi se bezbedna jednosmerna funkcija SHA (engl. *Secure Hash Algorithm, SHA*). Iz tako dobijene sažete verzije poruke generiše se digitalni potpis. Poruka se, zajedno sa pripadnim potpisom, šalje primaocu koji pomoću javnog ključa pošiljaoca utvrđuje verodostojnost poruke i samog digitalnog postupka. U postupku provere moraju se koristiti isti algoritmi za sažimanje poruka. Na slici 73 šematski su prikazani opisani postupci stvaranja i provere digitalnih potpisa.

Ukoliko se promeni sadržaj poruke, promeniće i potpis. Digitalni potpis se generiše na osnovu poruke koja se šalje, a potom šifruje tajnim ključem pošiljaoca i šalje zajedno sa porukom. Nakon prijema poruke primalac dešifruje potpis pošiljaoca njegovim javnim ključem. Zatim kreira potpis na osnovu poruke koju je primio i upoređuje ga sa primljenim potpisom. Ako su potpisi identični, utvrđuje da je ona stigla u nepromenjenom obliku (jer je utvrđeno da su potpisi identični).



Slika 73. *Šematski prikaz postupka stvaranja digitalnog potpisa*
Izvor: [626]

Procedura digitalnog potpisivanja koja se najčešće primenjuje u praksi je sledeća:

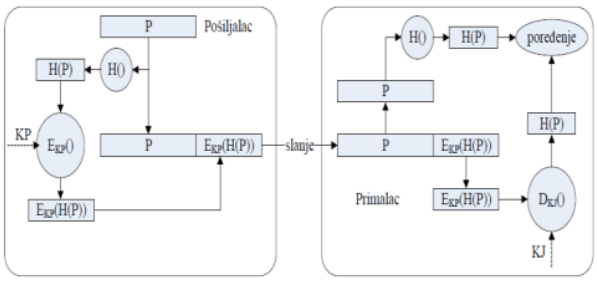
- Izračunava se jednosmerna *hash* vrednost dokumenta.
- Dobijena vrednost se propusti kroz funkciju čiji je parametar privatni ključ potpisnika.
- Kao rezultat se dobija digitalni potpis koji se čuva ili šalje zajedno sa dokumentom.

Procedura provere je:

- Verifikator izračunava jednosmernu *hash* vrednost dokumenta.
- Nad digitalnim potpisom se obavlja operacija koja je u suštini inverzna funkciji koju je obavio potpisnik i čiji je parametar javni ključ potpisnika.
- Dobijena vrednost treba da bude jednaka *hash* vrednosti dokumenta čime se potvrđuje da je potpis autentičan i da dokument nije izmenjen od potpisivanja.

Operacija koja se izvodi nad *hash* vrednošću dokumenta prilikom potpisivanja zavisi od izabranog algoritma za digitalni potpis. U praksi se najčešće koriste tri algoritma: RSA, ElGamal i DSA. Kod RSA algoritma potpisivanje predstavlja šifrovanje *hash*-a privatnim ključem, a verifikacija je dešifrovanje pomoću javnog ključa. [628] Kod ElGamal šeme potpisivanja koriste se posebni algoritmi za potpisivanje i verifikaciju, različiti od onog za šifrovanje i dešifrovanje, ali se i kod nje upotrebljava privatni ključ za potpisivanje, a javni za verifikaciju potpisa. [629] Algoritam DSA *(Digital Signature Algorithm, DSA)*, je standard vlade SAD i zasnovan je na Schnorri ElGamal algoritmima za digitalno potpisivanje. [630] Algoritam DSA je inicijalno definisao isključivu upotrebu SHA-1 heš funkcije, dok je kasnije dodata i SHA-2 heš funkcija. [631]

Treba naglasiti da digitalno potpisivanje ne predstavlja šifrovanje dokumenta i da su kriptografske namene digitalnog potpisa: integritet, potvrđivanje identiteta autora i neporicanje. Na potpisane dokumente ili poruke može se postaviti vremenska oznaka (engl. *timestamp*). Ovo se realizuje dodavanjem datuma i vremena u sadržaj dokumenta koji se hešira. Procedura potpisivanja korišćenjem RSA algoritma prikazana je na slici 74.



P – poruka
$H()$ – funkcija *hash*-ovanja
$H(P)$ – *hash* vrednost poruke
$E_{KP}()$ – funkcija šifrovanja ključem KP
KP – privatni ključ potpisnika
$E_{KP}(H(P))$ – digitalni potpis poruke
$D_{KJ}()$ – funkcija dešifrovanja ključem KJ
KJ – javni ključ potpisnika

Slika 74. *Procedura digitalnog poptisivanja i provere potpisa*
Izvor: [531]

8.2.4 Sertifikati i infrastruktura javnih ključeva

Možemo zaključiti da se kriptografijom sa javnim ključevima rešava problem bezbednog kanala za razmenu ključeva i broja ključeva potrebnih za bezbednu komunikaciju većeg broja lica. Ukoliko manji broj korisnika želi da međusobno komunicira koristeći šifarski sistem s javnim ključevima, oni se mogu razmeniti putem elektronske pošte, pomoću diskova ili USB memorije. Međutim, ako je grupa korisnika veća, ovakav način razmene ključeva nije praktičan. Isto tako, napadač može da podmetne svoj javni ključ i na taj način da čita šifrovane poruke namenjene drugim entitetima. [631]

Možemo zamisliti da dva lica (A i B) žele da koristeći kriptosistem s javnim ključem komuniciraju putem elektronske pošte. Tada lice A mora da poseduje javni ključ lica B ukoliko želi da mu pošalje poruku. Takođe, lice B mora da poseduje javni ključ lica A, ukoliko želi da mu pošalje poruku. Ovde se javlja problem integriteta njihovih javnih ključeva, odnosno, kako se može garantovati da je javni ključ lica B stvarno njegov, a ne ključ napadača koji želi da čita poruke lica A? Problem se rešava pomoću sertifikata i infrastrukture javnih ključeva. [632]

8.2.4.1 Digitalni sertifikati

Digitalni sertifikat (engl. *digital certificate*) možemo nazvati i digitalnom ličnom kartom za poslovanje u *cyber* prostoru. Ako u svojoj korespodenciji koristimo sistem šifrovanih poruka, i želimo nekom da pošaljemo poruku moramo da imamo njegov javni ključ. Za proveru identiteta pošiljaoca koristi se digitalni sertifikat. Digitalnim setifikat čine:

- naziv organizacije,
- javni ključ primaoca,
- informacije o identitetu (ime, identifikator korisnika – UID...),
- informacije vezane za ovlašćenja korisnika, npr. dozvole za pristup resursima (opciono),
- datum do kog važi vaš javni ključ,
- ime sertifikacionog tela koje je izdalo sertifikat,
- jedinstven serijski broj,
- jedan ili više digitalnih potpisa.

Ovi podaci se na kraju šifruju tajnim ključem sertifikacionog tela.

Verzija formata sertifikata
Serijski broj sertifikata
Identifikator algoritma kojim se vrši digitalni potpis
Naziv Sertifikacionog tela koje je izdalo sertifikat
Rok važnosti sertifikata
Naziv vlasnika sertifikata
Javni ključ vlasnika sertifikata
Određeni specifični podaci koji se odnose na uslove korišćenja sertifikata
DIGITALNI POTPIS SERTIFIKATA TAJNIM KLjUČEM SERTIFIKACIONOG TELA

Slika 75. *Sadržaj digitalnog sertifikata*
Izvor: [632]

Digitalnim sertifikatom se u web prostoru utvrđuje autentičnost lica ili kompanije potvrđivanjem njegovog sertifikata (javnog ključa). Digitalne sertifikate izdaje sertifikaciono telo (engl. *Cetificate Authority, CA*), posebna institucija koja je analogna MUP-u koji izdaje lične karte građanima. Sertifikaciono telo primenjuje savremene standarde za formiranje digatalnih sertifikata. Poverenjem u sertifikaciono telo i međusobnom razmenom sertifikata (javnih ključeva), stvara se sigurnost u sertifikate i njihovu ispravnost, tako da korisnici mogu verovati jedan drugome.

Digitalni potpis predstavlja potvrdu sertifikata. Njime se ne „overava" sertifikat u celini, već samo veza između identiteta korisnika i javnog ključa. U suštini, sertifikat je javni ključ sa opisom identiteta korisnika i potpisom koji je izdala strana kojoj se veruje, čime se potvrđuje veza između identiteta i ključa. Na taj način oni postaju identifikacioni sertifikati (engl. *identity certificate*) koji se koriste za identifikaciju pojedinaca, servera ili kompanija. Postoje i sertifikati akreditiva (engl. *credential certificate*) koji opisuju dozvole ili akreditive (npr. pristup određenom računaru).

Digitalni sertifikati pružaju podršku za:

- proveru identiteta,
- proveru integriteta,
- autorizaciju pristupa,
- neporecivost. [531]

Najćešće korišćeni standard za digitalne sertifikate je X.509 [633], koji definišu format *ISO* i *ITU-T* standard. [634] Format *X.509* podržava vodeći PKI – omogućeni protokoli i aplikacije kao što su *TLS/SSL*, *IPSec* i *S/MIME*.

8.2.4.2 Infrastruktura javnih ključeva

Infrastruktura javnih ključevima (engl. *Public Key Infrastructure, PKI*) obezbeđuje okruženje za pouzdanu primenu elekronskog poslovanja i najčešće se zasniva na kombinovanoj primeni asimetričnih i simetričnih šifarskih sistema. [635] Sastoji se od više elemenata, aplikacija i dokumenata koji definišu način implementacije četiri osnovne kriptografske funkcije u elektronskom poslovanju: zaštita tajnosti, autentičnost, integritet podataka i neporečivost transakcija. Potrebno je imati neku sertifikacionu ustanovu ili telo koje obezbeđuje javnu dostupnost digitalnih sertifikata.

Pomoću servera sertifikata (engl. *certificate server*) tj. baze podataka na mrežnom serveru obezbeđuje se sekundarna memorija za skladištenje sertifikata i mehanizmi za njihovu razmenu. Ne obezbeđuju mehanizme za izdavanje ili poništavanje sertifikata, već procedure samo za njihovo skladištenje i distribuciju – te se iz tog razloga ponekad nazivaju i skladišta sertifikata (engl. *certificate repositories*).

Za razliku njega, infrastruktura javnih ključeva predstavlja struktuirani sistem koji, osim skladištenja, pruža i dodatne funkcije za izdavanje i poništavanje sertifikata, kao i funkcije za uspostavljanje odnosa poverenja.

Tri osnovne komponente infrastrukture javnih ključeva su: sertifikacioni centar, registracioni centar i skladište sertifikata.

Sertifikacioni centar (engl. *Certificate Authority, CA*) – je potpisnik i izdavač sertifikata. Najvažnije funkcije CA su izdavanje sertifikata, njihovo obnavljanje i po potrebi opozivanje. Odgovoran je za generisanje sertifikata i njihov integritet. Svojim potpisom CA garantuje ispravnost podataka u sertifikatu. Ponekad CA obavlja i funkciju

bezbednosnog skladištenja ključeva. Upravo CA predstavlja izvor poverenja u PKI, a poverenje je osnova na kojoj se zasniva PKI. Primarnni zadatak ustanove koja obezbeđuje uslugu izdavanja digitalnih sertifikata jeste da bude poverljiva treća strana kojoj veruju učesnici u komunikaciji. Značajniji sertifikacioni centri su *Cybertrust GTE* (http://www.cybertrust.com), *VeriSign* (http://www.verisign.com) i *Thawte* (http://www.thawte.com). [632]

Registraciono telo (engl. *registration authority, RA*) – predstvalja autoritet u mreži koji proverava zahteve korisnika sa digitalnim sertifikatom i opcionalna je komponenta PKI. Uobičajena uloga mu je vezana za registraciju subjekata sertifikovanja. Navedene administrativne funkcije su obavezan deo PKI sistema i ako RA ne postoji, onda ih CA mora izvršavati samostalno. Funkcije koje RA ne može obavljati su izdavanje serifikata i staranje o listi opozvanih sertifikata.

U skladištu sertifikata se generišu javni ključevi i sertifikati korisnika, kao i tzv. liste opozvanih sertifikata (engl. *certificate revocation list,* CRL). Sertifikati moraju biti dostupni svim korisnicima PKI sistema. U tom pogledu se primenjuju skladišta sertifikata koja predstavljaju sistem ili skup distribuiranih sistema koji skladište sertifikate i liste opozvanih sertifikata i služe kao sredstvo za njihovu distribuciju krajnjim korisnicima. [633] Pod skladištima sertifikata se obično podrazumevaju X.500 direktorijumi. Skladišta mogu biti proste strukture kao što su obične datoteke na serveru dostupne preko *FTP* ili *HTTP* protokola. [636]

Sertifikati se izdaju sa periodom važenja, a mogu postati nevažeći i pre isticanja perioda važenja. Razlozi mogu biti: promena imena subjekta ili veze sa CA, ili bezbednosni kao što je kompromitovanje privatnog ključa subjekta. Liste opozvanih sertifikata (engl. *Certificate Revocation Lists, CRL*) predstavljaju uobičajen način objavljivanja opozvanih sertifikata zajedno sa razlogom za opozivanje. CRL lista je vremenski označena i identifikuje opozvane sertifikate potpisane od strane CA ili ovlašćenog izdavača CRL i slobodno dostupna u skladištu sertifikata. Svaki opozvani sertifikat je u CRL identifikovan svojim serijskim brojem. [637]

8.3 Upravljanje ključevima

Upravljanje ključevima je najteži deo kriptografije. [638] Isto tako, projektovanje bezbednih kriptografskih algoritama nije lako, ali se u svojim radovima možemo osloniti na obimna akademska istraživanja. [639] Držanje ključeva u tajnosti koji su osnovni element šifarskog sistema mnogo je teže. [640] To je razlog zašto je potrebno razmotriti pitanja njihovog skladištenja, dostupnosti ovlašćenim korisnicima sistema, način na koji se ključevi nađu kod ovlašćenih korisnika, kao i povezivanje ključeva sa subjektima, korisnicima sistema. [641] Ključevi mogu biti i otkriveni od strane neovlašćenih lica ili postati neupotrebljivi iz drugih razloga, pa je potrebno razmatrati i pitanje opozivanja ključeva.

Kriptoanalitičari često napadaju simetrične kriptosisteme i kriptosisteme sa javnim ključem kroz sam postupak upravljanja ključevima. Korisnici moraju da zaštite svoj ključ u meri koja je potrebna za podatke koji su šifrovani tim ključem. Ukoliko se ključ ne menja redovno, to može da bude ogromna količina podataka. [642]

Upravljanje ključevima odnosi se na bezbedno generisanje, distribuciju i čuvanje ključeva. Bezbednost samih metoda upravljanja ključevima ima veliku važnost. Nakon generisaanja ključa, on mora da ostane tajan da bi se izbegle situacije impersonalizacije.

Kada je reč o PKI sistemima, u praksi se najviše napada dešava na nivou upravljanja ključevima, dok su napadi na same algoritme retki. Učesnici u PKI sistemima moraju da imaju sposobnost generisanja ključeva. Takođe, korisnici moraju objavljivati svoj javni ključ i da imaju dostupnost javnih ključeva ostalih korisnika u sistemu, za šta se koriste sertifikati. Ukoliko dođe do kompromitovanja ili gubitka nečijeg privatnog ključa ostali učesnici moraju biti upozoreni, kako bi potencijalni napadač bio lišen mogućnosti dešifrovanja poruka koje su šifrovane odgovarajućim javnim ključem i mogućnosti neovlašćenog digitalnog potpisivanja. Korisnicima mora biti omogućeno da na bezbedan način čuvaju svoje ključeve i učine ih nedostupnim nelegitimnim korisnicima. [643]

Ključevi imaju ograničeno trajanje. Svoje postojanje ključ započinje generisanjem (kreiranjem), zatim prolazi fazu distribucije do korisnika i fazu čuvanja ključa do upotrebe, zatim se vrši upotreba ključa, onda eventualna zamena ključa zbog nedostataka odgovarajućim novim ključem i na kraju životni vek ključa se završava njegovim uništavanjem.

Najvažniji razlog za ograničeni životni vek ključa je zaštita od kriptoanalize. Svaki put prilikom upotrebe ključa generišu se šifrati koje napadač prikuplja i koristi ih za kriptoanalizu. Ukoliko vlasnik ključa posumnja da je napadač uspeo da dođe do ključa, treba razmotriti prestanak korišćenja kompromitovanog ključa i generisati novi ključ, odnosno novi par ključeva. Istraživanja u kriptoanalizi dovode do otkrivanja potencijalnih napada, pa se svakih nekoliko godina za pojedine algoritme povećava preporučena minimalna dužina ključeva.

8.3.1 Generisanje ključa

Već smo konstatovali da bezbednost algoritma počiva na ključu. Ukoliko se koristi slab postupak za generisanje ključeva, ceo šifarski sistem biće slab. U tom slučaju napadač ne mora da vrši kriptoanalizu algoritma za šifrovanje, već može da izvrši kriptoanalizu algoritma za generisanje ključeva. Upotreba pojedinih ključeva u određenim algoritmima za šifrovanje može se manifestovati nezadovoljavajućim karakteristikama ključeva.

Generisanje ključeva u šifarskim sistemima s javnim ključem je teže, jer ti ključevi često moraju imati određena matematička svojstva (prost broj, kvadratni ostatak...). Takođe, kada se koristi RSA algoritam brojeve p i q moramo birati iz skupa prostih brojeva. Neki ključevi se dobijaju i korišćenjem pseudo-slučajnih brojeva za šta je potrebno obezbediti generatore. Najbolji ključevi su slučajni ključevi, složeni onoliko teško koliko se teško pamte.

Većina šifarskih sistema obezbeđuje dosta metoda za generisanje ključeva. Uobičajen način je da sam korisnik izborom određene lozinke formira ključ. Korišćenjem nekog algoritma vrši se transformacija lozinke u ključ. Korisniku se tako omogućuje pamćenje jednostavne lozinke, umesto da pamti ključ velike dužine. Prilikom izbora lozinke preporučuje se uključivanje korišćenja brojeva i specijalnih karaktera. Lozinka dobijena korišćenjem brojeva i specijalnih karaktera u većem obimu smanjuje mogućnost otkrivanja ključa, a produžava vreme potrebno za njegovo otkrivanje. [644]

Kada lica sama biraju svoje ključeve obično vrše loš izbor. Najčešće se za ključ biraju imena supružnika ili se ključ zapisuje na papirić koji se nosi sa sobom. Ukoliko napadač koristi napad grubom silom on ne isprobava sve moguće ključeve u numeričkom redosledu, već testira očigledne ključeve. Ovakva vrsta napada naziva se napad pomoću rečnika (engl. *dictionary attack*). Napadač koristi rečnik uobičajenih reči u startu je u stanju da razbije 40% lozinki primenom ovakvog sistema kao što su ime korisnika, inicijali, ime naloga i druge značajne podatke kao moguću lozinku. [644] Takođe, napadač

može da koristi i reči iz različitih baza podataka, varijacije reči, strane reči, parove reči. Ova vrsta napada mnogo je efikasnija kada se koristi protiv datoteke ključeva, a ne jednog ključa.

Bolje rešenje je upotreba cele rečenice umesto jedne reči za konvertovanje u ključ. Ovakve rečenice nazivaju se lozinke fraze (engl. *pass phrases*). Tehnika obrada ključa (engl. *key crunching*) vrši konverziju rečenice koje se lako pamte u slučajne ključeve. Opisana tehnika se može koristiti u šifarskim sistemima s javnim ključem za generisanje privatnih ključeva gde bi se obradom teksta moglo dobiti slučajno seme koje bi se unosilo u deterministički sistem za generisanje parova javni – privatni ključ.

Preporuka Ministarstva odbrane SAD u generisanju slučajnih ključeva je korišćenje DES algoritma u režimu rada OFB (na osnovu vektorskih sistemskih prekida i sistemskih brojača). Preporuka je da se generiše DES ključ generisanjem inicijalizacionog vektora na osnovu radnog teksta, sistemskog ID, datuma i vremena. Za otvoreni tekst preporučuje se upotreba 64-bitni znakovni niz koji je generisan van sistema. Dobijeni rezultat se upotrebljava kao ključ.[645]

Dužina ključa predstavlja jednu od najbitnijih karakteristika koja se mora imati u vidu kada se generiše ključ. Određeni algoritmi koriste ključeve fiksne dužine, kao što je DES algoritam sa ključem od 56 bita. Najbolji slučaj je da korisnik može sam da izvrši izbor dužine ključa. Na svakih nekoliko godina povećava se preporučena minimalna dužina ključeva za pojedine algoritme.

8.3.2 Distribucija ključeva

Nakon završetka faze generisanja, ključevi se mogu primenjivati na različitim lokacijama i uz korišćenje raznolike opreme. Za svaki šifarski sistem važna je bezbedna distribucija ključeva kako bi se sprečila mogućnost presretanja od strane napadača koji bi mogao pročitati ili promeniti originalnu poruku. U cilju dopreme ključeva do udaljenih lokacija, oni se transportuju preko nezaštićenih komunikacionih kanala. Ako se ključevi tokom transporta ne zaštite, mogu biti ukradeni, što ceo šifarski sistem čini nebezbednim.

Jedno od rešenja koje se nameće je upotreba asimetrične kriptografije za razmenu sesijskih ključeva. Prepreka koja se ovde može javiti je takozvani napad presretanjem (engl. *man-in-the-middle attack*). Kod ovog napada napadač strani koja šalje sesijski ključ podmeće svoj javni ključ umesto javnog ključa onog kome se sesijski ključ šalje. Na ovaj način napadač može dešifrovati poruku sa sesijskim ključem, a pored toga može sesijski ključ šifrovati javnim ključem onoga kome je bio originalno poslan. Strane u konverzaciji ne bi bile ni svesne da je napadač došao do ključa kojim će oni šifrirati svoju komunikaciju. Način zaštite od ovakvih napada je obezbeđivanje uslova da javni ključ zaista pripada pravoj osobi što se ostvaruje sa infrastrukturom javnih ključeva (PKI).

Druga vrsta rešenja, zasnovana je na postojanju posrednika od poverenja sa kojim učesnici u komunikaciji imaju unapred razmenjene ključeve za simetričnu kriptografiju. Postoji nekoliko pitanja vezanih za rad i bezbednost ovog protokola. Prvo je da se protokol oslanja na apsolutnu pouzdanost posrednika. Posrednik treba da ima tajni ključ sa svakim od svojih korisnika i da omogući razmenu sesijskog ključa između bilo koja dva od njih. Uobičajeni termin za posrednika koji vrši ovu ulogu je Centar za distribuciju ključeva (engl. *Key Distribution Center, KDC*). On može postati preopterećen i postati usko grlo sistema. Takođe, pošto KDC zna sve ključeve u sistemu on postaje veoma privlačna meta za napadače. Pored ovih operativnih pitanja postoje i potencijalni bezbednosni propusti u ovom jednostavnom protokolu koji može dovesti do takozvanog napada ponavljanja (engl. *replay*). Napadač koji prisluškuje razmenu poruka može, i bez znanja sesijskog ključa,

ponovo poslati neku od poruka. Ovde napadač može iskustveno znati da je to poruka kojom se prijavljuje na sistem ili prenose neka novčana sredstva.

Da bi se otklonili ovi nedostaci razvijeno je više kriptografskih protokola za razmenu ključeva i potvrđivanje identiteta. U ovim protokolima koriste se dodatne veličine kao što su vremenske oznake (engl. *timestamp*) i slučajni brojevi koji obezbeđuju jedinstvenost (engl. *nonce*). Jedan od takvih je Needham-Schroeder protokol[646] koji obezbeđuje bezbedniju razmenu ključeva između entiteta kroz više naizmeničnih akcija razmena poruka tipa „izazov-odgovor". [598]

Rešenje je da se za distribuciju ključeva koriste bezbedni kanali, kao što je primera radi, dostavljanje ključa korisnicima putem pošte. Format zapisa ključa mora da bude razumljiv i univerzalan, tj. mora biti prepoznatljiv za svakog korisnika ili računar.

Ponekad tokom distribucije ključevi se oštete. Sve ključeve potrebno je prenositi sa nekom vrstom bitova za otkrivanje i ispravljanje grešaka. Time se mogu otkriti greške u prenošenju, i ako je to potrebno taj ključ se može poslati ponovo.[646] Najviše korišćena metoda je šifrovanje neke konstantne vrednosti sa ključem i slanje uz ključ 2 do 4 bajta tog šifrata, što se uradi i na strani primaoca. Ako se šifrovane konstante slažu, onda je prenošenje ključa izvršeno bez greške. Mogućnost ne otkrivanja greške je u intervalu od 1 prema 2^{16} do 1 prema 2^{32}.

8.3.3 Korišćenje ključeva

Korišćenje softvera za šifrovanje ključa veoma je problematično. Niko ne može garantovati da će operativni sistem na računaru privremeno prekinuti program koji upravo šifruje, sve upisati na disk i rešavati neki hitni zadatak. Kada se operativni sistem računara vrati na šifrovanje, bez obzira na sadržaj koji se šifruje, sve će izgledati da je u redu. Međutim, niko neće shvatiti da je operativni sistem računara upisao program za šifrovanje na disk računara i da je zajedno sa njime upisao i ključ. Taj ključ će se nalaziti na disku računara, nešifrovan, sve dok računar ne upiše nešto u toj zoni memorije. Vremenski period bi mogao da se meri minutima ili mesecima. Ključ bi se nalazio na disku kada bi pretpostavimo disk računara pretraživalo neovlašćeno lice. Ovo je razlog zašto je potrebno u višeprocesnoj obradi sa prekidima, operacijama šifrovanja dodeliti visoki prioritet kako ista ne bi mogla biti prekinuta.

Hardverske realizacije su bezbednije, jer mnogi uređaji za šifrovanje brišu ključ kada su napadnuti. Ovde je preduslov da mora da postoji poverenje u proizvođača hardvera, odnosno, da je implementirao određene jedinice koje omogućavaju ovakve i slične operacije.

Određeni komunikacioni programi kao što su programi za šifrovovanje telefonskih komunikacija, mogu da koriste sesijske ključeve. Oni se koriste samo za jednu komunikacionu sesiju, a zatim se odbacuju. Ovaj ključ se nakon toga više ne čuva. Isto tako, ukoliko se upotrebljava neki od protokola za razmenu ključeva u prenošenju ključa, taj ključ mora biti sačuvan pre korišćenja, što daje manju verovatnoću da će ključ biti otkriven. U određenim primenama poželjno je upravljati načinom korišćenja ključa sesije, jer pojedinim korisnicima mogu da budu potrebni ključevi sesije samo za šifrovanje ili samo za dešifrovanje. Ovi ključevi mogu biti raspoloživi za korišćenje na određenoj mašini ili u određeno vreme. Jedna šema za upravljanje ovim vrstama ograničenja pridružuje ključu upravljački vektor (engl. *control vector, CV*) koji definiše načine upotrebe i ograničenja tog ključa.[647][648] Prednosti se ogledaju u tome što upravljački vektor može biti proizvoljne dužine i uvek se skladišti uz šifrovani ključ, a pretpostavlja se otpornost hardvera i nemogućnost korisnika da direktno dođu do ključeva.

8.3.4 Skladištenje ključeva

S obzirom da su ključevi osnova bezbednosti u kriptografiji neophodno je njihovo čuvanje na bezbedan način. Sam ključ je niz bita i predstavlja podatak u digitalnom obliku. Za razliku od fizičkog ključa, krađu (kopiranje) digitalnog ključa teško je identifikovati.

Ključ koji se koristi za kriptografske operacije kad sa ne koristi mora biti skladišten na nekom medijumu, i dostupan u memoriji kada se koristi. U nekim sistemima primenjuje se jednostavan pristup: ključ se čuva u pamćenju nekog lica, a nikada u sistemu. Odgovornost tog lica je da pamti ključ i da ga unese svaki put kada treba da izvrši šifrovanje ili dešifrovanje neke datoteke. Primer ovakvog sistema je IPS.[649] Korisnik može neposredno da unese 64-bitni ključ ili da unese ključ kao dugi znakovi niz. Tada sistem primenom tehnike obrade ključeva, generiše 64-bitni ključ od tog znakovnog niza. Drugo rešenje je da se ključ skladišti na kartici, USB uređaju ili nekom drugom medijumu koje korisnik nosi sa sobom ili ih drži pod nekom fizičkom zaštitom. Pristup ključu na kartici je uglavnom zaštićen sa PIN. Za upotrebu ovakvih kartica potrebno je imati čitače koji se povezuju na računar koji se koristi za obavljanje kriptografskih operacija. Postoje i kartice koje pored memorije imaju i procesor za kriptografske operacije. Ovakve kartice obavljaju kriptografske operacije koristeći ključ koji je pohranjen na njima i time eliminišu potrebu da ključ ikad bude dostupan van kartice.

Dodatna mera zaštite, pored onih koje pružaju operativni sistemi, koja se ponekad koristi je da se za pristup datoteci sa ključem traži da korisnik unese tajnu informaciju koju samo on zna (lozinka, PIN) za koju se pretpostavlja da će je korisnik čuvati u glavi.

8.3.5 Zamena ključa

Kriptografski ključevi mogu biti kompromitovani, otkriveni od strane neovlašćenih lica ili postati neupotrebljivi iz drugih razloga. U takvim slučajevima neophodno je opozvati i zameniti ključ, odnosno proglasiti ga nevažećim, da bi se sprečila zloupotreba kompromitovanog ključa.

Kod opozivanja ključeva neophodno je kontrolisati da bude izvršeno na vreme i od strane ovlašćene osobe. Vreme koje protekne od kompromitovanja ključa pa do trenutka kada sve zainteresovane strane budu upoznate da je kompromitovani ključ nevažeći predstavlja vreme tokom koga je moguće izvršiti zloupotrebu ključa. Ovde se javlja potreba neophodnosti skraćivanja tog vremena. Neovlašćeno opozivanje ključa čini ključ bezrazložno neupotrebljivim. Obaveštenje o opozivanju ključa zato mora doći od lica koje je ovlašćeno za opozivanje tog ključa i mora se stvoriti mogućnost provere autentičnosti izvora i sadržaja poruke.

Svaki šifarski sistemi mora da ima mogućnost zamene ključa. Može postojati više razloga za zamenu, koje mogu biti planirane redovnim ažuriranjem ili zbog sumnji u ranije korišćene ključeve. Ako je reč o sumnji, zamena bi treba da bude izvedena u što kraćem vremenskom periodu. Redovnim ažuriranjem ključa smanjuje se mogućnost zloupotrebe.

Uspešnost napada direktno je proporcionalna vremenu i trudu koje napadač ulaže u cilju otkrivanja ključa. Na minimizaciju uspešnosti napada posebno utiču šifarski sistemi koji za svaku transakciju primenjuju različite ključeve (engl. *one time key*). U takvim sistemima napadač ulaže velike napore za otkrivanje ključa. Prelaskom na novu transakciju, šifarski sistem zamenjuje ključ, čime odvraća potencijalnog napadača od daljih pokušaja, produžavajući na taj način vreme potrebno za otkrivanje novog ključa za novu transakciju. Ako napadač poseduje jedan ključ, može dešifrovati samo jednu transakciju.

8.3.6 Uništavanje ključa

Ključ ima svoj vek trajanja. Često se upotrebljavaju ključevi koji su namenjeni samo za jednu transakciju. Na kraju nje se ključ uništava i više se ne može koristiti. Neki ključevi se moraju redovno menjati, a stari ključevi uništiti. Isto tako, neki ključevi se mogu sertifikovati za određeni vremenski period. Treba napomenuti da su stari ključevi vredni bez obzira na to što se više ne koriste. Ako napadač dođe do starih ključeva, on može da pročita stare poruke koje su šifrovane tim ključem. [650] Oni se moraju uništiti na bezbedan način.

Mogući problem predstavlja mogućnost kopiranja i upisivanja ključeva u računar na više mesta. Svaki računar koji upravlja svojom memorijom tako što neprekidno prebacuje programe u memoriju i iz memorije, usložava ovaj problem. Potrebno je razmisliti o pisanju posebnog programa za brisanje ključeva, koji skenira sve diskove, tražeći kopije šablona bitova ključa ili neupotrebljene blokove, a zatim ih briše. Takođe, potrebno je nastojati da se izbrišu sadržaji privremenih datoteka na računaru ili datoteka za razmenu podataka.

Prilikom prenosa, ključ može da se izgubi ili ošteti. U tom slučaju, vlasnik ključa mora da upozori ostale korisnike da ključ više nije validan i da se više ne sme primenjivati. Oštećenjem ili kompromitacijom para ključeva, ne moraju se obaveštavati svi korisnici ključeva, naročito ako se ključevi čuvaju na serveru. Periodičnim pretraživanjem podataka na serveru može se dobiti informacija o ključevima koji su van upotrebe. Kada se utvrdi koji ključevi nisu u upotrebi, pristupa se uništavanju, ali se informacija o uništenju ključa čuva na serveru sve dok ne istekne originalni sertifikat. Upravo ove karakteristike čine asimetrične sisteme pogodnim za korišćenje na Internetu.

9. Studija slučaja: Kriptografska rešenja zaštite projektovanog integrisanog automatizovanog sistema upravljanja memorije organizacije

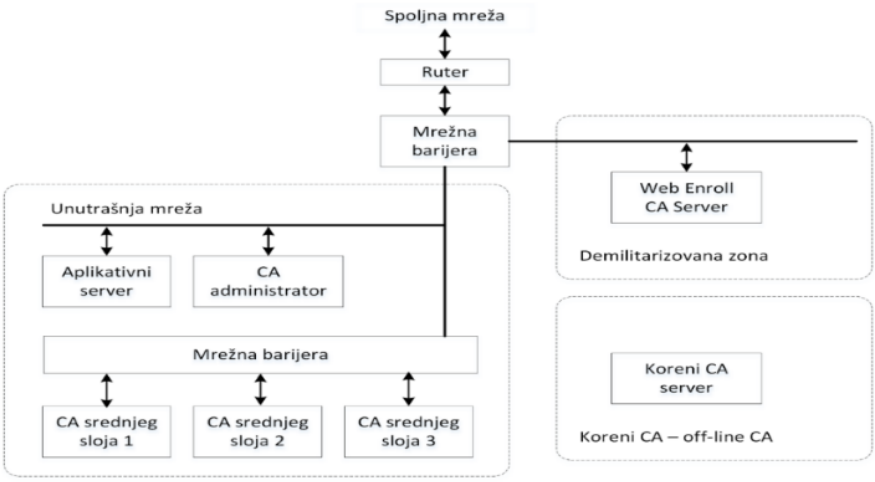
9.1 Uvod

U ovom poglavlju je dat predlog jednog rešenja kriptografske zaštite projektovanog integrisanog automatizovanog sistema upravljanja memorije organizacije. Predložen pristup zaštiti prethodno pomenutog sistema u obzir uzima infrastrukturu javnih ključeva zasnovanu na *Microsoft* tehnologiji i primenu pametnih kartica. Na osnovu toga je definisano rešenje zasnovano na upotebi korporativnih identifikacionih kartica u informacionom sistemu kompanije. Zaštitni mehanizmi koji se predlažu obuhvataju višeslojnu arhitekturu zaštite na aplikativnom, transportnom i mrežnom sloju, jake mehanizme kontrole pristupa (kao što je dvofaktorska autentifikacija i autorizacija zasnovane na definisanim ulogama povezanim sa korisničkim grupama u Aktivnom Direktorijumu (engl. *Active Directory*), kao i neke mehanizme zaštite baza podataka informacionog sistema kompanije koji otkrivaju i sprečavaju curenje podataka iz analitičkih sistema. Kritički osvrt na dato rešenje, dat je na kraju ovog poglavlja rada.

Kompanije imaju unutrašnje i spoljašnje korisnike. U unutrašnje korisnike spadaju zaposleni, dok se pod pojmom spoljašnji korisnici podrazumevaju korisnici u užem smislu te reči i, eventualno, partneri kompanije (drugim rečima, druge kompanije koje sarađuju sa kompanijom). Ovakve kompanije svoje infrastrukture javnih ključeva mogu da realizuju upotrebom *Microsoft* sertifikacionog tela za unutrašnje korisnike, dok se za izdavanje sertifikata za spoljašnje korisnike može koristiti posebno privatno sertifikaciono telo. Primena *Microsoft* zasnovanih servisa koji se odnose na sertifikate predlaže se iz razloga ekonomičnosti i mogućnosti domenske integracije, odnosno mogućnost integracije sa Aktivnim Direktorijumom. Potrebno je napomenuti da se mogućnost integracije odnosi na takozvanu *Enterprise*, ali ne i na *Standalone* varijantu, koja predstavlja jeftinije rešenje koje je, pored zasebnih sertifikacionih tela, takođe prikladno za spoljašnje korisnike. Što se ekonomičnosti tiče, potrebno je naglasiti da su sertifikacioni servisi uključeni u samu licencu servera, te da ne postoje posebne licence koje se odnose na sertifikate, što drugim rečima znači da nema dodatnih troškova. Pre same implementacije *Microsoft* sertifikacionih servisa u informacionom sistemu kompanije (organizacije), potrebno je definisati hijerarhiju sertifikacionih tela, odnosno definisati broj nivoa u okviru hijerarhije i broj tela na svakom nivou, kao i tipove sertifikata koje će svako od prethodno pomenutih tela izdavati. Takođe, treba uzeti i potrebu za različitim politikama sertifikacije. Jedno od mogućih rešenja predstavlja hijerarhija na dva nivoa. U slučaju da se radi o zatvorenoj grupi sa spoljašnjim korisnicima, dovoljno je koristiti jedno sertifikaciono telo (engl. *root CA*) i dva podređena tzv. *Subordinate CA* za unutrašnje i spoljašnje korisnike. Ukoliko postoji potreba da sertikati spoljašnjih korisnika budu kvalifikovani, sertifikaciono telo koje im izdaje sertifikate mora biti akreditovano shodno zakonskim regulativama koje se odnose na izdavanje kvalifikovanih sertifikata.

Predlog rešenja opisanih u ovom poglavlju, zasnivaju se na izdavanju sertifikata na pametnim karticama za unutrašnje korisnike – sertifikate izdaje koreni autoritet koji je integrisan sa Aktivnim Direktorijumom. Time se korisnicima omogućava zaštićeno prijavljivanje na računare sa operativnim sistemom *Windows* koji su učlanjeni u domen u okviru informacionog sistema, upotreba kriptografski zaštićene elektronske pošte na *Microsoft* klijentima za elektronsku poštu i autentifikacija klijenata prilikom pristupa

pojedinim Web servisima koje su zaštićeni protokolom SSL (engl. *Secure Sockets Layer*). Ukoliko postoji potreba za izdavanjem kvalifikovanih sertifikata spoljašnjim korisnicima, unutrašnji korisnici koji komuniciraju putem kvalifikovanog digitalnog potpisa sa spoljašnjim korisnicima, osim nekvalifikovanog sertifikata za pristup domenskim servisima na pametnim karticama moraju imati i kvalifikovan sertifikat za prethodno pomenutu komunikaciju. Arhitektura predloženog sistema infrastrukture javnih ključeva sastoji se od različitih komponenata koje se nalaze u različitim bezbednosnim zonama, kao što su unutrašnje zone, demilitarizovane zone i slično. Na primer, server za izdavanje sertifikata Web servisima (*Web Enroll CA*) smešten je u demilitarizovanoj zoni, aplikativni server u unutrašnjoj zoni dok su *CA* serveri srednjeg sloja (engl. *intermediate CA*) smešteni u unutrašnjoj zoni višeg bezbednosnog nivoa (slika 76).



Slika 76. *Arhitektura predloženog sistema za upravljanje sertifikatima*
Izvor: Autor

Komunikacija između prethodno pomenutih komponenti sistema mora da bude kriptografski zaštićena upotrebom protokola SSL, pri čemu se u protokolu insistira na obostranoj autentifikaciji, odnosno autentifikaciji servera klijentu, kao i autentifikaciji klijenta serveru putem digitalnog sertifikata izdatog za odgovarajuće servis na datom serveru. Treba naglasiti i da je koreni server u potpunosti odvojen i nije povezan ni na jednu lokalnu mrežu. Takođe, u predloženom rešenju postoje i neke administrativne aplikacije koje se odnose na infrastrukturu javnih ključeva, kao što su operator registracionog autoriteta (RAO) i operator sertifikacionog autoriteta (CAO) koje pristupaju preko unutrašnje mreže namenskom Web servisu na aplikativnom serveru. I u ovom slučaju, pristup je kriptografski zaštićen protokolom SSL koji uključuje autentifikaciju klijenta serveru zasnovanu na sertifikatu izdatom na pametnoj kartici administratora, a kao dodatna zaštitna mera uvodi se ograničenje koji se odnosi na pristup administrativnoj aplikaciji samo sa radne stanice administratora.

U okviru sistema infrastrukture javnih ključeva, pametne kartice treba da obezbede sledeće funkcionalnosti: generisanje para ključeva i bezbedno čuvanje istih i generisanje digitalnog potpisa. Takođe, potrebno je naglasiti da su kartice zaštićene od neovlašćenog čitanja podataka (na primer, privatni ključ ne može biti iščitan sa kartice, a sama kartica se u tom slučaju ponaša kao tzv. *tamperproof* modul). Da bi se pametne kartice mogle primeniti u sistemu infrastrukture javnih ključeva, neophodno je da se poseduje sledeće: pametna kartica sa čipom koji omogućava primenu algoritama sa javnim ključem,

aplikacija koja prihvata veći broj parova sertifikata – privatni ključ koji se nalazi na samoj kartici, čitač kartica sa odgovarajućim veznikom (engl. *driver*), pri čemu se zahteva podrška za veći broj različitih verzija operativnih sistema familije *Windows*, i softver srednjeg sloja koji najčešće obezbeđuje sam proizvođač operativnih sistema za pametne kartice. Ovaj softver obično sadrži: davaoca kriptografskih usluga (engl. *cryptographic service provider*) koji omogućava *Microsoft* aplikacijama da koriste karticu, biblioteke koje omogućavaju aplikacijama koje se ne oslanjaju na Microsoft komponente da koriste karticu i odgovarajuće upravljače za administriranje kartice (na primer, pregled sadržaja, izmena PIN broja i slično). Sertifikate unutrašnjim korisnicima izdaje sertifikacioni autoritet na osnovu para ključeva koji su prethodno generisani na samoj kartici.

9.2 Profilisanje sertifikata koji će se upotrebljavati u PKI sistemu

Da bi se iskoristile sve prednosti *Microsoft* sertifikacionog autoriteta, neophodno je dobro osmisliti profile sertifikata koji će se koristiti u u okviru datog sistema infrastrukture javnih ključeva. Da bi korisnici pametnih kartica sa izdatim sertifikatom mogli da koriste funkcionlosti prijavljivanja na *Windows* operativne sisteme, zaštićenu elektronsku poštu i zaštitu podataka upotrebom SSL protokola i klijentske autentifikacije, sertifikat mora da sadrži sledeća proširenja:

- Prijavljivanje na sistem – proširenja AIA i CDP, vrednost *Smart Card Logon* (prijavljivanje putem pametne kartice) unetu u proširenje *Enhanced Key Usage* (proširena upotreba ključa), i domensko ime korisnika uneto u polje *Principal Name* (ime principal) u okviru proširenja *Subject Alternative Name* (alternativno ime subjekta).
- Upotreba zaštićene e-pošte – proširenja AIA, CDP i S-MIME *Capabilities*, uključena adresa e-pošte u strukturu *Subject* korisnika (polje označeno oznakom E), adresa e-pošte uključena u proširenje *Subject Alternative Name* (ovo je alterantiva prethodnom zahtevu) i primena vrednosti *Secure Email* (zaštićena e-pošta) u proširenju *Enhanced Key Usage*.
- Zaštita podataka upotrebom SSL protokola i klijentske autentifikacije – zahteva se navedena vrednost*Client Authentication* (autentifikacija klijenta) u proširenju *Enhanced Key Usage*.

Jedan od šablona koji obezbeđuje dovoljan broj korisnih funkcionalnosti je *Smart Card User* šablon (šablon korisnika pametne kartice).[651] Ovaj šablon karakteriše proširenje *Key Usage* koje sadrži vrednosti *Digital Signature* (digitalni potpis) i *Key Encipherement* (šifrovanje ključa), kao i sledeća proširenja koja su uključena u sertifikat:

- proširenje S-MIME *Capabilities*,
- proširenje *Certificate Template Name* (ime šablona sertifikata) sa vrednošću *Smartcard User* (korisnik pametne kartice),
- proširenja AIA i CDP,
- proširenje *Enhanced Key Usage* sa podešenim vrednostima parametara za upotrebu zaštićene elektronske pošte (*Secure Email*), autentifikacije klijenta (*Client Authentication*) i prijavljivanje pomoću pametne kartice (*Smart Card Logon*),

- proširenje *Subject Alternative Name* u kome je upisano ime domenskog korisnika u polje *Principal Name* (ime principala) i adresa elektronske pošte u polje *RFC822 Name*.

Korisnici informacionog sistema kompanije sa pametnim karticama na kojima su generisani parovi ključeva (privatni i javni ključ – pri čemu još jednom napominjemo da se privatni ključ ne može neautorizovano iščitati sa kartice), koji na svojim računarima imaju instalirane čitače pametnih kartica i odgovarajući softver, kao sertifikate izdate od domenski vezanog korenog autoriteta izrađene na osnovu *Smart Card User* šablona, mogu koristiti sledeće funkcionalnosti: prijavljivanje na *Windows* operativne sisteme, zaštićenu elektronsku poštu u slučaju da koriste *Microsoft* klijente za e-poštu, kao što su *Outlook* i *Outlook Express* i zaštitu podataka koji se prenose preko mreže na transportnom sloju upotrebom SSL protokola i klijentske autentifikacije. Drugim rečima, dobra osobina ovog rešenja leži u tome što se upotrebom korenog sertifikacionog autoriteta i izdavanjem sertifikata po prethodno pomenutom šablonu za unutrašnje korisnike omogućava jednostavno korišćenje zaštitnih mehanizama bez potrebe za instaliranjem dodatnog softvera (isključujući veznik za čitač pametnih kartica).

9.3 Upotreba korporativnih identifikacionih kartica u informacionom sistemu

U ovom delu rada daje se predlog osnovnih karakteristika potencijalnog rešenja primene korporativnih identifikacionih kartica u informacionom sistemu kompanije.

Korporativna identifikaciona kartica je identifikuje zaposlenog u kompaniji. Ona služi za implementaciju logičke bezbednosti unutar informacionog sistema kompanije, a po potrebi i fizičke bezbednosti. Čip pametne kartice može da generiše i čuva par ključeva (privatni i javni ključ), pri čemu kartica treba da ima najmanje tri slobodna para ključeva, kao i da generiše digitalni potpis. Pri tome, prvi par ključeva i sertifikat izdat od unutrašnjeg sertifikacionog autoriteta koristi se za prijavljivanje na računare koji se nalaze u domenu, upotrebu zaštićene elektronske pošte i klijentsku SSL autentifikaciju. Osnovna ideja je sprovođenje politike prijavljivanja na sistem na osnovu dvo-faktorske autentifikacije (nešto što imamo – pametna kartica, i nešto što znamo – PIN broj) i sprečavanje prijavljivanja pomoću domenskog korisničkog imena i lozinke (jedno-faktorska autentifikacija), čime se značajno povećava nivo bezbednosti u samoj infrastrukturi koja podržava informacioni sistem kompanije. Drugi par ključeva može da bude slobodan za dalje primene, a može, ukoliko za tim postoji potreba, da se iskoristi kao kvalifikovani digitalni sertifikat koji je izdalo sertifikaciono telo ovlašćeno za izdavanje istih. Treći par ključeva treba da ostane slobodan za eventualne primene u budućnosti. Osim toga, poželjno je da kartica ima beskontaktni čip za potrebe fizičke kontrole pristupa, koji se može iskoristiti za kontrolu pristupa određenim prostorijama.

Da rezimiramo, osnovne komponente predloženog sistema su:

- pametne kartice sa minimum tri para ključeva (privatni i javni) najmanje dužine 2048 bita i odgovarajućom aplikacijom za rad sa infrastrukturom javnih ključeva smeštenom na karticama,
- odgovarajući softveri za rad sa aplikacijama na prethodno predloženim karticama koji se mora realizovati na svim klijentskim računarima,
- čitači pametnih kartica,
- infrastruktura javnih ključeva zasnovana na *Microsoft* PKI tehnologiji koja obuhvata odgovarajuće procedure registracije korisnika,

- softver za upravljanje pametnim karticama koji bi se koristio u okviru sistema infrastrukture javnih ključeva i
- fizička kontrola pristupa u pojedinim prostorijama kompanije primenom beskontaktnih čitača kartica (smeštenih na ulasku u prostorije organizacije), kontrolera za upravljanje čitača i odgovarajućeg softvera za centralizovano nadgledanje sistema. Sistem bi trebalo integrisati sa postojećim projektom uvođenja sistema fizičke kontrole pristupa.

9.4 Višeslojna arhitektura zaštite komunikacionih kanala u okviru informacionog sistema kompanije

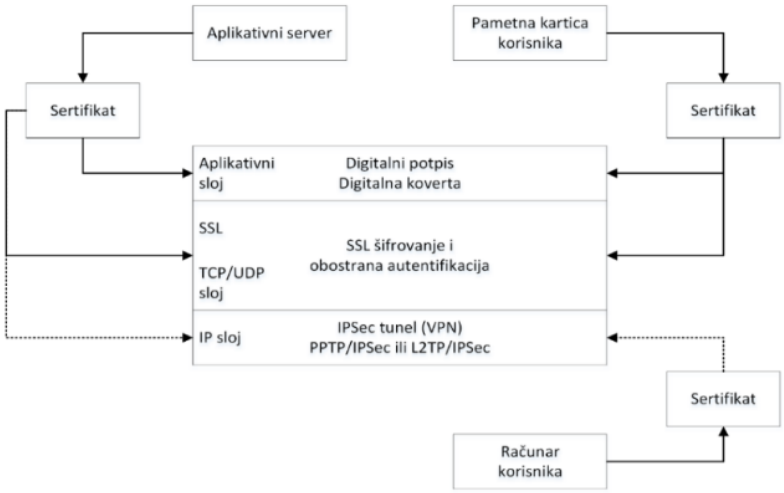
U cilju implementacije optimalne zaštite u informacionom sistemu kompanije od potencijalnih pretnji i napada kojima mogu biti izloženi različiti servisi i resursi, predlaže se primena arhitektura sistema zaštite sastavljena od mehanizama zaštite primenjenih na tri nezavisna bezbednosna nivoa, odnosno sloja TCP/IP skupa protokola:

- zaštita na aplikativnom sloju,
- zaštita na transportnom sloju i
- zaštita na mrežnom IP sloju.

Predlog je zasnovan na preporuci istovremene primene mehanizama zaštite na više različitih nivoa OSI referentnog modela. Ako je korišćenje mehanizama na svim nivoima nemoguće, predlaže se primena kombinacija mehanizama na bar dva sloja: zaštita na aplikativnom sloju, kao obavezna i dodatna zaštita na transportnom ili mrežnom nivou. Time se obezbeđuje zaštita sistema od napada iznutra (aplikativni sloj) i spolja (transportni ili mrežni sloj).

Zaštita na aplikativnom sloju zasnovana je na primeni tehnologije digitalnog potpisa na temeljima algoritama sa javnim ključem i zaštite privatnosti podataka primenom simetričnih šifarskih algoritama. Ovaj nivo zaštite se može posmatrati kao linija odbrane od napada iznutra (engl. *insider attack*) i obezbeđuje: proveru autentičnosti korisnika servisa, štićenje integriteta podataka koji se prenose, zaštitu od mogućnosti naknadnog poricanja odgovornosti za poslate podatke i zaštitu privatnosti podataka. U cilju realizacije mehanizama zaštite na aplikativnom sloju predlaže se primena digitalnog potpisa i digitalne koverte (engl. *envelope*) zasnovane na primeni pametnih kartica. Kako bi se implementirala zaštita na ovom nivou, neophodno je instalirati odgovarajuće kriptografske komponente na klijentu (u okviru odgovarajuće klijentske aplikacije ili čitača Web) i serveru koje su zadužene za realizaciju kriptografskih funkcija na aplikativnom sloju. Navodimo neke od karakterisika kriptografskih komponenti koje su neophodne. Komponenta treba da obezbedi fukncije provere autentičnosti korisnika, integriteta datoteka, neporecivosti i zaštite privatnosti podataka. U tom smislu koriste se simetrični algoritmi, algoritmi sa javnim ključem, digitalni potpis i generisanje ključeva na pametnim karticama. Određene kriptografske funkcije, kao što je digitalni potpis i dešifrovanja simetričnog ključa pri upotrebi digitalne koverte izvršavaju se na samoj kartici, dok se ostale izvršavaju na klijentskom i serverskom softveru. Takođe, kriptografske komponente trebaju da imaju mogućnost provere digitalnog potpisa podataka na osnovu javnog ključa sertifikata potpisnika i proveru samog sertifikata koji je stigao uz poruku, što podrazumeva proveru da li je sertifikat izdat od strane autoriteta sa poverenjem, da li je sertifikat istekao ili je povučen, odnosno da li se nalazi na listi povučenih sertifikata koju izdaje sertifikacioni autoritet (engl. *certificate revocation list, CRL*). Što se usklađenosti sa

standardima tiče, očekuje se usklađenost sa sledećim standardima: *PKCS#1* [652] za digitalni potpis i kovertu, *PKCS#7* [653] za format zaštićenih podataka i *PKCS#11* [654] standardni interfejs za pristup pametnim karticama. Biblioteka treba da bude univerzalna u odnosu na pametne kartice i čitače pametnih kartica – drugim rečima ne sme se vezati za konkretan model ili konkretnog proizvođača. Na taj način se obezbeđuje nezavisnost klijentske i serverske aplikacije od konkretne pametne kartice koja se koristi za prelaz na drugi tip kartice, i prateće uređaje za očitavanje istih je relativno jednostavan. Biblioteka mora da obezbedi funkciju provere autentičnosti korisnika na osnovu njegove pametne kartice i PIN broja a pre nego što se omogući korišćenje same aplikacije. Drugim rečima, aplikacija ne može da se pokrene bez upotrebne odgovarajuće pametne kartice ovlašćenog korisnika, unošenja PIN broja i provere validnosti sertifikata korisnika. Klijentska aplikacija treba da omogući odabir sertifikata korisnika koji potpisuje poruku ili datoteku (u slučaju da računar koristi više korisnika), kao i odabir sertifikata primaoca (nalaze se u repozitorijumu sertifikata drugih korisnika u okviru Aktivnog Direktorijuma), prikaz informacija o podacima koji se digitalno potpisuju, prikaz informacije o tome da li je digitalno potpisivanje, odnosno šifrovanje podataka uspešno ili ne, kao i prikaz informacija o tome da li je provera digitalnog potpisa, odnosno procedura dešifrovanja podataka uspešno ili neuspešno obavljena. Kriptografska komponenta na klijentu i serveru treba da podrži veliki broj simetričnih i asimetričnih algoritama koji obavljaju operacije šifrovanja i dešifrovanja sa različitim dužinama ključeva, kao i heš funkcija, a da pri tome postoji mogućnost implementacije novih algoritama, kao i zamene onih za koje postoji opravdana sumnja ili je teorijski dokazano da su kriptografski slabi (na primer, postoji napad kojim se složenost u odnosu na napad potpunom pretragom značajno smanjuje). Aplikacija treba da osigura promenu dužina odgovarajućih ključeva ako za tim postoji potreba.



Slika 77. *Višeslojna arhitektura zaštite komunikacionih kanala u okviru informacionog sistema kompanije*
Izvor: Autor

Zaštita privatnosti podataka primenom simetričnih šifarskih algoritama i autentifikacije čvornih tačaka (engl. *node*) komunikacionog segmenta mreže na transportnom nivou predstavlja zaštitu na transportnom nivou. Na ovom sloju mreža se štiti od napada spolja (engl. *outsider attack*) primenom šifrovanih tunela između čvornih tačaka komunikacije u mreži na transportnom nivou primenom simetrične kriptografije i procedura jake autentifikacije između čvorišta mreže čime se osigurava provera autentičnosti strana u komunikaciji. Što se tiče implementacije transportnih mehanizama

zaštite, predlaže se primena standardnog protokola SSL. Moguće su dve osnovne konfiguracije protokola: SSL sa autentifikacijom servera klijentu i SSL sa obostranom autentikacijom na osnovu digitalnih sertifikata i pametnig kartica korisnika (u oba slučaja je neophodno da npr. Web servis ima validan SSL sertifikat). U informacionom sistemu kompanije predlaže se primena protokola SSL sa autentifikacijom klijenta serveru i servera klijentu. Drugim rečima, predlaže se zaštita na transportnom sloju i jaka autentifikacija korisnika na bazi protokola SSL sa obostranom autentifikacijom zasnovanom na primeni pametnih kartica korisnika i na izdatih digitalnih sertifikata. Ovim se postiže da samo klijenti sa pametnim karticama i validnim sertifikatima mogu da ostvare pristup datom serveru, a samim tim i da izvršavaju odgovarajuće poslovne procese u okviru informacionog sistema kompanije.

Zaštita na nivou Internet protokola (odgovara mrežnom sloju u *ISO/OSI* referentnom modelu) obezbeđuje logičku zaštitu na nivou *IP* paketa. Ovaj vid zaštite zasniva se na ostvarivanju *IPSec* tunela, odnosno formiranju virtuelnih privatnih mreža (engl. *Virtual Private Network, VPN*). Pristup poslovnih jedinica koje ne komuniciraju putem mreže koja se nalazi u vlasništvu kompanije omogućava se pomoću VPN tunela tipa sajt-prema-sajtu, pri čemu se tunel, odnosno šifrovanje na mrežnom sloju, okončava na spoljnom interfejsu mrežne barijere. Za potrebe pristupa korisnika spolja, ili korisnika iznutra koji ostvaruju udaljen pristup potrebno je upostaviti *PPTP/IPSec* ili *L2TP/IPSec* putem odgovarajuće VPN metode. U okviru informacionog sistema kompanije predlaže se primena *IPSec* protokola na bazi digitalnih sertifikata čvornih tačaka u računarskoj mreži, ili između klijenta i VPN servera. Na taj način VPN mreža se može se uspostaviti između dva uređaja (ruteri ili mrežne barijere) ili između VPN klijenta i koncentratora na osnovu digitalnih sertifikata.

9.5 Jaka kontrola pristupa i mehanizmi zaštite informacionog sistema kompanije

U ovom poglavlju, predstavljen je koncept realizacije sistema zaštite informacionog sistema kompanije. Koncept se zasniva na realizaciji odgovarajućih zaštitnih mehanizama koji su projektovani da ispune zahteve sistema bezbednosti savremenih informacionih sistema. Mehanizmi zaštite u okviru informacionog sistema kompanije su:

- mehanizmi jake kontrole pristupa (dvo-faktorska autentifikacija i autorizacija korisnika zasnovana na ulogama povezanim sa grupama u aktivnom direktorijumu) i
- mehanizmi zaštite baza podataka informacionog sistema kompanije koji otkrivaju i sprečavaju curenje podataka (engl. *data leak*) iz analitičkih sistema (engl. *online analytical processing*, OLAP) stvaranjem kanala zaključivanja.

Osnovne pretpostavke na osnovu koji se predlaže realizacija zaštite su date u nastavku teksta. Web aplikacije koje se koriste u organizaciji su aplikacije troslojne arhitekture čiji su elementi Web server, aplikativni server i server baze podataka. Korisnici mogu da pristupe informacionim sistemima putem Web pregledača, specifične aplikacije koja pristupa serverskoj aplikaciji putem SOAP protokola ili klijentske aplikacije u klijent-server arhitekturi. U sistemu treba da bude realizovana procedura dvofaktorske autentifikacije korisnika, zasnovane na pametnim karticama, kako za korišćenje sistema putem Web pregledača tako i za korišćenje putem namenske aplikacije. U slučaju da korisnik pristupa preko Web čitača, onda se autentikacija vrši na serverskoj strani. Ukoliko se radi o namenskoj aplikaciji onda se korisnik autetnifikuje kako za pristup datoj aplikaciji na klijentskoj strani, tako i na serverskoj strani. U okviru kompanije neophodno

je da se prethodno formira sertifikaciono telo (sistem infrastrukture javnih ključeva). U sistemu se primenjuje sistem više nivoa kriptografske zaštite (vidi poglavlje 9.4) na sledećim slojevima:

- aplikativni (digitalni potpis i koverta),
- transportni (protokol SSL protokol) i
- mrežni (protokol IPsec).

Aplikacije treba da omoguće i eventualnu integraciju sa operativnim sistemom Windows i da poseduju sopstvene sisteme autorizacije korisnika zasnovanih na ulogama. Na kraju, potrebno je omogućiti naknadnu integraciju informacionog sistema kompanije sa drugim informacionim sistemim, ukoliko za to postoji potreba. Što se tiče zaštite baza podataka, potrebno ih je zaštiti od potencijalnih zloupotreba koje se odnose na curenja podataka iz analitičkih sistema stvaranjem kanala zaključivanja, a takođe se mogu uvesti dodatne kriptografske mere zaštite poverljivih podataka.

Mehanizmi koji se predlažu za primenu u okviru sistema zaštite zasnivaju se na: infrastrukturi javnih ključeva, digitalnim sertifikatima i pametnim karticama za unutrašnje korisnike. U nastavku su izložene karakteristike predloženih mehanizama zaštite.

9.5.1 Predlog rešenja jake kontrole pristupa

Kako bi korisnici pristupili odgovarajućoj aplikaciji informacionog sistema potrebno je definisati postupke identifikacije, autentifikacije i autorizacije korisnika. Identifikacija se najčešće realizuje primenom jednoznačnog identifikatora u sistemu, kao što je na primer korisničko ime. Autentifikacija se realizuje korišćenjem lozinke ili digitalnog sertifikata izdatog od strane davaoca sertifikata u sistemu infrastrukture javnih ključeva. Autorizacija korisnika najčešće se vrši tako što se proveri kojoj ulozi (engl. *role*) u sistemu pripada korisnik, a zatim se proveravaju prava koja data uloga ima na sistemu. U moguće vidove autentifikacije korisnika u informacionom sistemu organizacije spadaju korisničko ime i lozinka, korisničko ime i jednokratna lozinka (engl. *one-time password, OTP*), i upotreba jake dvofaktorske autentifikacije zasnovane na infrastrukturi javnih ključeva i pametnim karticama.

Implementacija jake autentifikacije korisnika u informacionom sistemu kompanije može se realizovati na dva načina. Prvi način je autentifikacija korisnika u operativnom sistemu *Windows*. Tada se pretpostavlja da se za potrebe autentifikacije korisnika u operativnom sistemu koristi jaka dvo-faktorska autentifikacija zasnovana na pametnim karticama. Drugi način je kombinovanje jednostavne autentifikacije u operativnom sistemu i SSL klijentske dvo-faktorske autentifikacije korisnika za pristup samim aplikacijama informacionog sistema kompanije na osnovu digitalnog sertifikata i pametne kartice. Oba pomenuta rešenja jake autentifikacije korisnika u aplikacijama informacionog sistema ne zahtevaju od korisnika unos korisničkog imena i lozinke za pristup samoj aplikaciji jer se ti podaci nalaze u Aktivnom Direktorijumu, a autentifikaciju korisnika vrši operativni sistem Windows ili, kombinovano, operativni sistem i protokol SSL implementiran u samoj aplikaciji. Napominjemo da korisnici za pristup aplikaciji mogu da koriste Web pregledač ili samostalnu klijentsku aplikaciju.

Aplikacije informacionih sistema kompanije treba da poseduju sopstveni sistem autorizacije korisnika zasnovan na ulogama i da obezbede eventualnu integraciju sa operativnim sistemima u cilju autorizacije korisnika. Definisanjem uloga, kao i dodelom adekvatnih prava u aplikaciji za svaki tip korisnika, od strane administratora informacionog sistema ili aplikacije obezbeđuju se uslovi za bezbedan rad aplikacija.

Što se tiče korisnika inicijalno se mogu definisati sledeće uloge: administratori, unutrašnji korisnici sistema i spoljašni korisnici sistema. Administratori su korisnici sa svim pravima u sistemu, koji mogu da upravljaju sistemom, kao i da ažuriraju korisnike i uloge u sistemu (na primer, kreiranje novih uloga, izmena prava postojećih, uparivanje korisnika sa ulogama i slično). Unutrašnjim korisnicima se dodeljuju odgovarajuća prava pregleda i ažuriranja informacija i dokumenata koji se čuvaju u informacionom sistemu. Spoljašnji korisnici predstavljaju korisnike kojima kompanija pruža različite usluge. Pored navedenih mogu se definisati i dodatne uloge.

Postupak autorizacije korisnika u potpunosti treba zasnivati na kontroli pristupa putem Aktivnog Direktorijuma. Administratori sistema u tom slučaju mogu povezati uloge korisnika sa odgovarajućim grupama u Aktivnom Direktorijumu koje su namenski kreirane i namenjene za potrebe informacionog sistema. Postavljanjem korisnika u odgovarajuću grupu u Aktivnom Direktorijumu istovremeno mu se dodeljuju i odgovarajuća prava u različitim aplikacijama. Administraciju korisnika i definisanje prava mogu da realizuju dva administratora: administrator Aktivnog Direktorijuma i administrator informacionog sistema kompanije. Ove dve funkcije administratora ne bi trebalo da obavlja jedna osoba. Broj uloga u sistemu, kao i njihove mogućnosti definišu se tokom razvoja informacionog sistema. Pri tome, potrebno je omogućiti da neki korisnici imaju više od jedne uloge u sistemu.

9.5.2 Konkretni predlozi potencijalnog rešenja realizacije sistema zaštite informacionog sistema kompanije

U okviru ovog poglavlja se predlažu konkretni mehanizmi višeslojne arhitekture zaštite za realizaciju.

U odnosu na potrebe korisnika, predlaže se primena sledećih mehanizama zaštite:

- za administratora sistema (korišćenje kombinovanih mehanizama zaštite na transportnom i aplikativnom nivou),
- za korisnike sistema (korišćenih kombinovanih mehanizama zaštite na transportnom i aplikativnom nivou).

Mehanizme zaštite na transportnom sloju predstavlja protokol SSL, sa autentifikacijom od klijenta ka serveru i od servera ka klijentu. Navedeni tipovi korisnika treba da poseduju pametne kartice na kojima je generisan i smešten privatni ključ za asimetrični šifarski algoritam i digitalni sertifikat. Korisnik se može autentifikovati prema Web serveru ili servisu i za to koristiti ili sertifikat (Web aplikacije) ili takozvani otisak svog sertifikata (heksadecimalni niz koji jedinstveno identifikuje sertifikat, engl. *certificate thumbprint*), zajedno sa sertifikatom (Web servis). U slučaju klijentske autentikacije na neki Web servis sa SSL zasnovanom komunikacijom, tada sertifikat korisnika treba da, pored pametne kartice, bude i na direktorijumu samostalne aplikacije koja služi za eventualni poziv Web servisa ili se autentikacija sertifikata korisnika koji može da pristupi vrši na bazi otiska njegovog sertifikata. Serverski SSL sertifikat treba da generiše odgovarajuće sertifikaciono telo, pri čemu dužina kluča treba da bude najmanje 2048 bita.

Zaštita na aplikativnom nivou između korisnika i servera na osnovu digitalnog potpisa i pametnih kartica korisnika, moguće je implementirati na dva načina.

- U prvom slučaju, korisnik upotrebljava Web pregledač, autentifikuje se na osnovu pametne kartice i SSL klijentske autentifikacije, a zatim koristi mehanizme zaštite na aplikativnom sloju za zaštitu datoteka ili HTML strana koje se dostavljaju do Web, odnosno aplikativnog servera.

- U drugom slučaju, korisnik primenjuje samostalnu klijentsku aplikaciju u kojoj se autentifikuje pametnom karticom i izdatim digitalnim sertifikatom. Komunikacija aplikacije sa Web serverom se implementira preko Web servisa koji se izvršavaju na Web serveru. Kao mehanizam zaštite na aplikativnom nivou primenjuju se digitalni potpisi i koverte, kao i protokol SSL sa klijentskom autentifikacijom između aplikacije i Web servisa na strani Web servera.

Za algoritme i dužine ključeva predlaže se sledeća primena: asimetrični privatni ključ korisnika (dužine najmanje 2048 bita, generisan na pametnoj kartici), algoritam sa javnim ključem (RSA), heš algoritam (najmanje SHA-2, poželjno SHA-3), simetrični algoritam (AES sa dužinom ključa 256 bita), SSL serverski sertifikat, asimetrični par ključeva serverskog SSL sertifikata (1024 bita) i simetrični algoritam u SSL protokolu (RC4 sa dužinom ključa 128 bita ili jači).

Sva dokumenta koja se razmenjuju unutar informacionog sistema organizacije moraju biti digitalno potpisana, a pojedina dokumenta (koji imaju odgovarajući stepen tajnosti i poverljivosti) moraju biti i šifrovana putem digitalne koverte.

Treba napomenuti da se sprovodi dvostruko šifrovanje: digitalnom kovertom na aplikativnom sloju i primenom protokola SSL na transportnom sloju. Obzirom da se SSL šifrovanje završava na Web serveru lociranom u tzv. demilitarizovanoj zoni, a aplikativno šifrovanje završava na aplikativnom serveru u unutrašnjoj zoni. Osim toga, šifrovanje digitalnom kovertom je procedura šifrovanja za namenjenog primaoca (u ovom slučaju aplikativni server) i niko drugi tu poruku ne može da dešifruje.

U ovom slučaju, procedura zaštite bi se mogla realizovati uspostavljanjem SSL sesije sa Web serverom na osnovu autentifikacije klijenta digitalnim sertifikatom koji se nalazi na pametnoj kartici, a zatim se u okviru klijentske aplikacije (ili Web pregledaču) obavi digitalni potpis i kreira digitalna koverta poruke odnosno datoteke koja se šalje.

Za navedeno, potrebno je da Web i aplikativni server poseduju odgovarajuće kriptografske komponente za realizaciju mehanizama aplikativne zaštite sa funkcijama koje su obrađene u nastavku teksta. Kriptografska komponenta na Web serveru verifikuje digitalni potpis dostavljenih podataka i validira korisnikov sertifikat. Ako je validacija uspešna, Web server vrši prosleđivanje kompletno dostavljenih podataka do aplikativnog servera kako bi oni bili obrađeni i smešteni u bazu podataka kompanije. Kriptografska komponenta vrši dešifrovanje podataka na aplikativnom serveru ukoliko je korisnik primenio postupak kreiranja digitalne koverte. Aplikativni server treba da poseduje osim kriptografske komponente i odgovarajuću pametnu karticu u kojoj se nalazi privatni ključ za dešifrovanje podataka. Podaci se čuvaju u otvorenom ili šifrovanom obliku u bazi podataka informacionog sistema kompanije, u zavisnosti od stepena tajnosti datih podataka i predviđenog načina čuvanja podataka sa datim stepenom tajnosti. Što se tiče pametne kartice i asimetričnih ključeva aplikativnog servera, primenjuju se isti zahtevi kao i za korisnike s jednom izmenom – asimetrični ključ je generisan, a zatim je napravljena rezervna kopija spolja i naknadno je upisan na pametnu karticu. Razlog ove izmene je mogućnost oporavka ključa u slučaju kvara pametne kartice.

Obzirom da se u informacionim sistemima najčešće primenjuje SOA arhitektura i da aplikativni slojevi komuniciraju putem Web servisa, svaki od servera generiše i koristi dva SSL sertifikata (serverski i klijentski). Između svaka dva servera u arhitekturi (Web server – aplikativni server, aplikativni server – server koji pristupa podacima) se uspostavlja se SSL protokol sa klijentskom i serverskom autentifikacijom. Time se povećava nivo bezbednosti čitavog sistema zato što se pomenuti serveri međusobno

autentifikuju, a čitava komunikacija je nakanadno šifrovana kroz uspostavljene kriptografske tunele.

Administrator primenjuje pametnu karticu za potrebe digitalnog potpisivanja svih aktivnosti koje obavlja a koje se odnose na informacioni sistem kompanije. Tako se sve akcije koje su izvršene od strane administratora, čuvaju se u bazi podataka sistema uz digitalni potpis administratora. U normalnim okolnostima, administrator ne bi trebalo da vrši digitalni potpis informacija, odnosno dokumenata koji se unose u sistem.

9.5.3 Neki mehanizmi zaštita baza podataka i sprečavanja curenja podataka iz analitičkih sistema

Zaštita baza podataka informacionog sistema kompanije – memorije organizacije zasniva se na nekoliko mehanizama. Osnovna zaštita baza podataka zasnovana je na standardnim mehanizmima zaštite koji su ugrađeni u sam sistem za upravljanje bazama podataka, odnosno serverskoj komponenti, kao što je *Microsoft SQL servera* (na primer, ovlašćenja, kaskadna autorizacija sa vremenskom sinhronizacijom, upotreba uloga, pogleda, uskladištenih procedura i okidača). Baze podataka u sistemu kakav je memorija organizacije koji sadrže dokumenta, odnosno informacije sa određenim stepenom tajnosti treba zaštititi upotrebom šifrovanja na način na koji je opisano u prethodnim poglavljima ovog rada. Time se sprečava pristup podacima za korisnike sa nižim nivoom ovlašćenja, a takođe se može i evidentirati svaki uspešni pokušaj pristupa, kao i neuspešni, odnosno pokušaj korisnika sa nižim nivoom ovlašćenja (kao što su spoljašnji korisnici) da pristupi podacima višeg stepena tajnosti (jedan od načina otkrivanja curenja podataka). Ovaj način kontrole pristupa odgovara jednostavnom svojstvu sigurnosti u *Bell – LaPadula* modelu kontrole pristupa, pri čemu se zvezdica svojstvo bezbednosti može implementirati prema potrebi. Drugim rečima, sistem treba da obezbedi evidentiranje svih važnih događaja u bazi podataka uz odgovarajući digitalni potpis unosa u dnevničku datoteku od strane operatera ili administratora koji je izvršio transakciju. Osim toga, potrebno je sprečiti kanal zaključivanja i curenje podataka koje se može stvoriti u statističkim bazama podataka memorije organizacije koje se koriste uglavnom u analitičke svrhe. Statistička baza je takozavani *OLAP* sistem (engl. *online analytical processing*, *OLAP*) za razliku od klasične baze koja je *OLTP* (engl. *online transaction processing*, *OLTP*) sistem. Za razliku od čistih statističkih baza koje sadrže podatke u statističkom obliku (poput proseka, najvećih vrednosti, i slično), što znači da ne postoji mogućnost krađe, odnosno curenja nestatističkih podataka, standardne baze podataka sa statističkim pristupom su ranjive na krađu nestatističkih podataka.

U ovom slučaju, neprivilegovani korisnici i spoljašnji korisnici sistema imaju pravo obraćanja bazi podataka samo preko statističkih upita, dok privilegovani korisnici pristupaju bazi na nivou diskrecione kontrole pristupa, obavezne kontrole pristupa ili RBAC (engl. *role based access control*, *RBAC*) prava pristupa. Sprečavanje kanala zaključivanja u statističkim bazama može se izvršiti restrikcijom upita. Na primer, baza podataka može da odgovori samo na strogo statističke upite neprivilegovanim korisnicima, pri čemu se zabranjuju isuviše selektivne *WHERE* klauzule i koriste inteligentni agenti za otkrivanje nedozvoljene upotrebe sistema. Osim toga, predlaže se podela baza na disjunktne delove, čime se značajno otežava dobijanje korisnih statističkih podataka i dodavanje šuma (baza podataka obezbeđuje odgovor na sve upite, ali je odgovor približan).

9.5.4 Kritički osvrt na predloženo rešenje i smernice za dalja istraživanja

Predloženo rešenje zaštite integrisanog automatizovanog sistema upravljanja memorije organizacije uzima u obzir infrastrukturu javnih ključeva zasnovanu na

Microsoft tehnologiji i primenu pametnih kartica. Na osnovu toga definisano je rešenje zasnovano na upotebi korporativnih identifikacionih kartica u informacionom sistemu memorije organizacije kompanije, pri čemu zaštitni mehanizmi koji se predlažu obuhvataju višeslojnu arhitekturu zaštite na aplikativnom, transportnom i mrežnom sloju, jake mehanizme kontrole pristupa kao i neke mehanizme zaštite baza podataka informacionog sistema kompanije koji otkrivaju i sprečavaju curenje podataka iz analitičkih sistema.

Na osnovu izloženog se može zaključiti sledeće:

- Autentifikacija korisnika je dvo-faktorska. Klijent bez važećeg sertifikata smeštenog na pametnoj kartici nema prisup aplikaciji, a samim tim ni podacima u informacionom sistemu kompanije.
- Autorizacija korisnika je integrisana sa Aktivnim Direktorijumom, a administrativne dužnosti su podeljene na administraciju Aktivnog Direktorijuma i administraciju samog informacionog sistema kompanije, što značajno olakšava administraciju korisnika i uloga.
- Šifrovanje podataka obavlja se na dva nivoa: pomoću digitalne koverte i pomoću protokola SSL sa obostranom autentifikacijom zasnovanom na digitalnim sertifikatima smeštenim na pametnim karticama.
- Curenje osetljivih podataka iz analitičkih sistema i baza podataka memorije organizacije sprečava se dodavanjem šuma u odgovoru koji baza vraća korisniku, šifrovanjem podataka u transakcionim sistemima, onemogućavanjem određenog broja upita transakcionim sistemima spoljašnjim korisnicima i vođenjem dnevnika u kome je svaki zapis digitalno potpisan ključem koji se nalazi na pametnoj kartici.

Ukoliko se predloženi sistem kritički analizira, mogu se uočiti dva fundamentalna ograničenja.

- Prvo ograničenje predloženog rešenja je u tome što je sistem čvrsto vezan za *Microsoft* platformu, što znači da se aplikacije moraju razvijati za date operativne sisteme ili eventualno *Java* platformu (u opštem smislu može dovesti do određenih bezbednosnih propusta).
- Drugo ograničenje ogleda se u mogućnosti zloupotrebe kartice u slučaju kompromitovanja PIN broja, što kroz obezbeđene usluge neporecivosti usled digitalnog potpisa na osnovu ključa sa pametne kartice može dovesti do izvesnih pravnih problema usmerenih ka vlasniku kartice. Drugim rečima, ukoliko neko iskoristi pametnu karticu legitimnog korisnika (pod uslovom da poznaje PIN broj), zapis u dnevničkoj datoteci će biti digitalno potpisan ključem sa kartice, što legitimni korisnik ne može (ukoliko nije prijavio krađu kartice) da demantuje, odnosno opovrgne. U slučaju da je krađa prijavljena, neophodno je izdati novu karticu, drugi sertifikat i nove parove ključeva korisniku.

Shodno uočenim ograničenjima, smernice za dalji rad predloženog sistema mogu se rezimirati u sledećim crtama.

- Predloženo rešenje treba generalizovati, odnosno ponuditi radni okvir pogodan za implementaciju za sve operativne sisteme. Na taj način moguće je iskoristiti

rešenja otvorenog koda čime bi se značajno smanjili troškovi licenciranja (naročito za serversku familiju *Microsoft* operativnih sistema).

- Pametne kartice se u predloženom rešenju štite PIN brojem. Kao što je već pomenuto, krađa kartice i PIN broja može rezultovati digitalno potpisanim unosom u dnevničkoj datoteci koji korisnik ne može da opovrgne. U tom smislu se predlaže upotreba biometrije (na primer, otiska prsta) u dvo-faktorskoj autentifikaciji umesto upotrebe PIN-broja, čime bi se sprečila moguća zloupotreba kartica u slučaju krađe i kompromitovanja PIN broja.

9.5.5 Hipotetičko rešenje datog problema

Predlog rešenja na lokalnom nivou

Ovo rešenje čine tri celine: klijentska strana, server za autentifikaciju i server za rad sa bazom podataka.Ostvarivanje komunikacije između klijenta i servera za autentifikaciju, odnosno servera za rad sa bazom podataka vrši se preko strane klijenta. Ona ima dve funkcije:

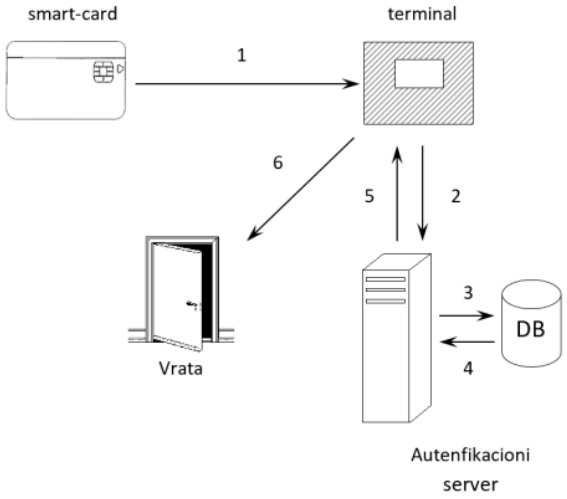
- prilikom prijavljivanja na sistem vrši pripremu parametara za pristup u odgovarajući paket i prosleđuje ga serveru za autentifikaciju,
- prilikom pristupa bazi podataka vrši pripremu paketa za komunikaciju sa serverom za rad sa bazom.

Osnovni uslov za ostvarivanje komunikacije sa serverom za autentifikaciju je generisanje para ključeva od strane klijenta. Tom prilikom vrši se primena asimetrične kriptografije. Šifrovanje poruke vrši se javnim ključem, dok jedino privatni ključ tu poruku može da dešifruje. Šifrat ne može da se dešifruje javnim ključem, tako da iz javnog ključa ne može da se rekonstruiše privatni ključ. Međutim, iz privatnog ključa može da se rekonstruiše javni ključ. Osnovna ideja ovog rešenja je da svaki klijent u sistemu ima svoj par ključeva, odnosno da server za autetntifikaciju ima par ključeva za svakog klijenta. Razmena ključa vrši se u oba smera. Klijent serveru za autentifikaciju prosleđuje svoj javni ključ, a server za autentifikaciju prosleđuje kljentu njegov generisani javni ključ. Prednost koju pruža ovakav način komunikacije ogleda se u tome da ne postoji opasnost da napadač presretne javni ključ.

Osnovni zahtev za implementaciju ovog načina rada je čuvanje parametara na strani servera za autentifikaciju. Pristupni parametri čuvaju se u bazi podataka memorije organizacije u koju server za autentifikaciju ima mogućnost da upiše par ključeva, vreme kreiranja i vreme isteka (vremenski pečat), i identifikaciju koji je klijent zahtevao pristup. Ključni deo ovog protokola predstavlja izdavanje tiketa ili ulaznice, koji su od ključnog značaja, jer u sebi sadrže ključeve i druge informacije koje su potrebne za pristup bazama podataka. Mogu biti privremene ili odobrene. Prvi tiket je privremeni i generiše se prvi put kada korisnik zahteva rad sa bazom podataka, odnosno kada se zahteva proces autentifikacije. Ovaj tiket omogućava razmenu ključeva između servera za autentifikaciju i korisnika. On je osnova za prosleđivanje korisničkih kredencijala od korisnika do servera za autentifikaciju korišćenjem asimetrične kriptografije.

Kada se uspešno izvrši autentifikacija, odnosno kada server za autentifikaciju dešifruje privatnim ključem za datog korisnika i proveri parametre, generiše se odobreni tiket koji u sebi nosi parametre (simetrični ključ i jedinstveni identifikator) za pristup serveru i rad sa bazom podataka. Odobreni tiket šifrovan sa klijentovim javnim ključem se prosleđuje klijentu, tako da napadač ne može da ga snimi, koristi i dešifruje. Ovim principom komunikacije i načinom razmene ključeva osigurava se integritet privatnosti i

integritet podataka.



Slika 78. *Arhitektura zaštite komunikacionih kanala u okviru informacionog sistema kompanije na lokalnom nivou*
Izvor: Autor

Primer 1. Pretpostavimo da imamo neku smart karticu (tiket, ulaznica) na kojoj imamo upisane određene informacije, kao što su jedinstveni identifikator korisnika i kodovani *helper data* koji se odnosi na javni ključ izdat za tog korisnika, generisan na osnovu biometrijskih podataka korisnika.

Kada korisnik prinese svoju karticu terminalu, terminal očita jedinstveni identifikator i šifrat i to prosledi serveru za autentifikaciju.

Server za autentifikaciju pronalazi u lokalnoj bazi podataka kodovani privatni ključ, ekstrahuje privatni ključ na osnovu priložene biometrije i dešifruje šifrat na osnovu koga vrši autentifikaciju korisnika. Privatni ključ je zaštićen biometrijskim templejtom korisnika. Ista biometrija se koristi za obezbeđivanje sigurnosti privatnog i javnog ključa datog korisnika. Ukoliko je autentifikacija uspešna, sve što autentifikacioni server treba da uradi je da prosledi neku vrstu flag-a ili signala terminalu da otključa vrata ili ukoliko se radi o pristupu radnoj stanici, samu radnu stanicu. Kako bi se sprečila mogućnost lažiranja ili fabrikovanja signala prema terminalu mogu se uvesti mere zaštite slanja signala kao što je izazov–odgovor, kriptografske zaštite slanja signala pomoću jednom korišćenjih ključeva itd.

Možemo zaključiti sledeće: Smart kartica na kojoj je upisan jedinstveni identifikator korisnika i lozinka za pristup sistemu šifrovana izdati su javnim ključem, dok je privatni ključ sačuvan u bazi podataka.

Autentifikacioni server dešifruje šifrat tako što u bazi podataka pronalazi privatni ključ i vrši autentifikaciju korisnika. Ovde treba napomenuti da su cela baza podataka ili neophodne kolone šifrovane master ključem tako da ni administrator ne može da čita ključeve.

Predlog rešenja za udaljeni pristup

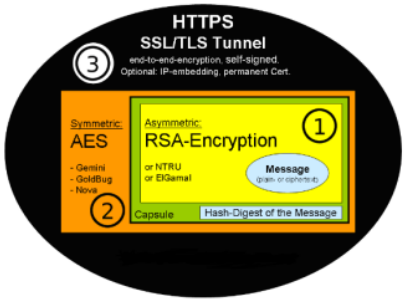
U ovom slučaju, predlažemo sledeći princip. Ukoliko imamo korisnika koji želi da koristi svoju radnu stanicu ili otvori vrata, on će za to koristiti svoju smart karticu (tiket, ulaznicu). Ovo je princip da se autentifikacija vrši na osnovu nečega što imamo vezano za

klijenta. Ukoliko je ovo nedovoljno, možemo iskoristi još nešto dodatno kao što je biometrijski podataka klijenta (otisak prsta, skeniranje irisa, glas, hod i sl.) ili nešto drugo što znamo (PIN kod).

Nakon izvršenog prvog koraka lokalnom serveru za autentifikaciju prosleđuju se sledeće informacije:

- jedinstveni identifikator korisnika,
- PIN / biometrija (otisak prsta skeniranje irisa, glas, hod i sl) i
- šifra sa smart kartice

Pitanje koje se ovde postavljaje je da li želimo da informacije koje se prenose do lokalnog servera za autentifikaciju budu šifrovane na neki način ili ne. Moramo imati u vidu da ukoliko je napadač u zgradi i na primer, da je pustio *Wireshark* kako bi snimio komunikaciju kroz mrežu, on je u mogućnosti da snimi informacije o PIN-u ili otisku prsta klijenta. U ovom delu postupka obavezno je izvršiti primenu neke vrste šifrovanja (upotrebe određenih protokola). Predlažemo upotrebu SSL protokola.



Slika 79. *Format šifrovane poruke*
Izvor: Adams/Maier (2016), GoldBug Study

Uzmimo za primer veliku kompaniju koja ima dosta svojih poslovnica. Lokalni server za autentifikaciju sadrži informacije o zaposlenima samo u toj lokalnoj poslovnici. Ukoliko u kompaniju dolazi gost ili zaposleni iz druge poslovnice, lokalni server će za autentifikaciju morati da izvrši konekciju na Internet i pošalje upit glavnom serveru za autentifikaciju za informacije o korisnicima. Ovde je potrebno napomenuti da ovi lokalni serveri za autentifikaciju nemaju admina i u njihove baze podataka ne može da se vrši upisivanje nezavisno od glavnog servera za autentifikaciju. Kada imamo novog zaposlenog njegove informacije se upisuju u glavni server za autentifikaciju, a onda ostali lokalni serveri povlače te informacije i čuvaju ih u svojim bazama podataka. Ovakvim postupkom vrši se izbegavanje velikih razlika u sistemu. Glavni server uvek može da informiše lokalne servere za autentifikaciju da osveže svoje baze podataka sa novim informacijama.

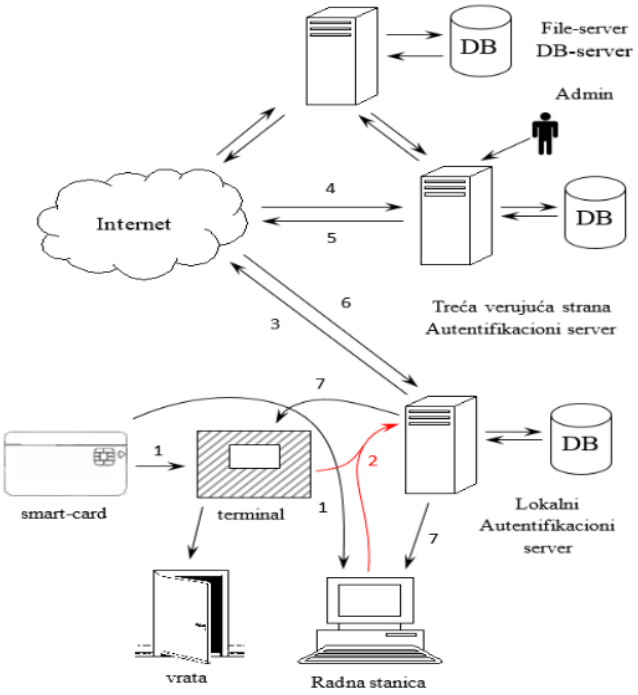
Ovde se javlja potreba neophodnosti uspostavljanja sinhronizacije baze podataka na lokalnom i udaljenom serveru za autentifikaciju. Algoritmi i protokoli koji bi mogli da se koriste u ovom slučaju su:

- SSL protokol, sa svim sigurnosnim zakrpama koje sprečavaju moguće napade na sigurnosne propuste otkrivene od 2014. do 2016. godine, kao što je napad tipa FREAK itd.,
- Kerberos,
- AES algoritam sa ključem, 256 u CBC režimu i sa PKCS7 padding-om,
- RSA algoritam, sa ključem dužine 2048 bita,

- SHA-3 heš funkcija, koji generiše heš dužine 512 bita sa dodatkom kriptografske soli (engl. *salt*).

Kako bi izbegli mogućnost curenja ključeva i osetljivih informacija, kao i napad grubom silom može se limitirati vreme trajanje jedne sesije na 30 minuta nakon čega će se zahtevati ponovna autentifikacija korisnika. Dodatno server za autentifikaciju će po svakoj autentifikaciji generisati novi ključ za tu komunikaciju, a prethodni ključ će se označiti kao da je istekao.

Što se tiče master ključa kojim se šifruje baza podataka, on može da se generiše jednom dnevno ili na mesečnom nivou gde će se čitava baza prethodno dešifrovati na osnovu starog, a potom šifrovati sa novim ključem. A ako ne želimo da šifrujemo čitavu bazu možemo je delimično šifrovati (kolone sa privatnim ključevima i generisanim aktivnim sesijskim ključevima).



Slika 80. *Arhitektura zaštite komunikacionih kanala u okviru informacionog sistema kompanije korišćenjem Interneta (udaljeni pristup)*
Izvor: Autor

Primer 2. Opis po koracima (slika 80).

1. Prinosimo smart karticu terminalu. Terminal očitava podatke sa smart kartice i prosleđuje lokalnom serveru za autentifikaciju.
2. Lokalni server za autentifikaciju proverava prispele podatke da li se poklapaju sa onima koji se nalaze u lokalnoj bazi podataka. Ukoliko takav zapis ne postoji u lokalnoj bazi podataka šalje se zahtev za novim podacima iz glavnog servera za autentifikaciju.
3. Slanje zahteva za novim podacima sa glavnog servera za autentifikaciju.
4. Ovaj korak predstavlja nastavak koraka 3.
5. Odgovor glavnog servera za autentifikaciju.
6. Nastavak odgovora.

7. Odgovor lokalnog servera za autentifikaciju da se otključa radna stanica ili vrata ukoliko je autentifikacija uspešna.

Opciona modifikacija je ukoliko se radi zahtev za resursima sa fajl servera ili servera baze podataka na internetu. Treba obezbediti distribuciju ključeva sa lokalnog servera odnosno glavnog servera za autentifikaciju i šifrovati upite odnosno odgovore fajl servera ili servera baze podataka.

10. Zaključak

Analizirajući dosadašnja iskustva u radu modernih kompanija (organizacija) kada je u pitanju bezbedan pristup i korišćenje informacija i resursa memorije organizacije (znanja kompanije), ključni izazov za u 21. veku predstavlja način na koji kompanije pristupaju, koriste, skladište i čuvaju svoje znanje. Ali isto tako i na koji način zaboravljaju to znanje koje poseduju. Postavlja se pitanje i gde kompanije na osnovu upravljanja znanjem – memorijom organizacije, zadržavaju i skladište svoje informacije, odnosno na koji način organizuju i na kojim principima uspostavljaju memoriju organizacije. Ovo je veoma značajno, jer se u uspešnom radu svake kompnije podrazumeva ponovno korišćenje informacija - znanja kompanije. Znanje kojim bilo koja kompanija raspolaže uvek se može na tržištu pretvoriti u novu vrednost kompanije. Uspešnost svake kompanije predstavlja i razvijena praksa upravljanja znanjem (memorijom organizacije) čime se omogućava dostupnost ekspertskog znanja za brzo i efikasno i kvalitetna rešavanja poslovnih problema, a čime se doprinosi povećanju tržišne vrednosti i konkurentnosti na tržištu. Isto tako, veoma važno je i kako se primenjuju iskustva, da li su stečena, nasleđena ili kupljena, a zatim način na koji će se ta iskustva koristiti u praksi. Na kraju potrebno je i odrediti se prema načinu kako se postupa sa uskladištenim informacijama i memorijom rganizacije.

Ovim radom kriptografska rešenja zaštita memorije organizacije sa stanovišta menadžmenta znanja želi se dobiti i određenje ne samo da li je potrebno upravljati znanjem – memorijom organizacije, već i na koji način treba pristupati, skladištiti, čuvati i kako upravljati memorijom organizacije.

Kako bi se blagovremeno zaštitile informacije koje su same po sebi vitalne i veoma važne za kompaniju potrebno je slediti princip da sam predloženi protokol kriptografske zaštite memorije organizacije sa stanovišta menadžmenta znanja zahteva da protokol bude bezbedan. Ovim principom se vrši onemogućavanje eventualnog napadača da pristupi informacijama u realnom vremenu, ili da izazove trošenje većih vrednosti resursa napadača od vrednosti samih informacija do kojih napadač želi da pristupi.

Sam napadač može da dođe do informacija kroz snimanje komunikacije između klijenta i servera za autentifikaciju, odnosno servera za rad sa bazom podataka memorije organizacije. Kada se snima komunikacija klijenta i servera za autentifikaciju napadač može doći do inicijalne poruke koju svaki učesnik može da inicira u sistemu i ona nema neku posebnu važnost, jer se kreira za svakog klijenta nezavisno i ne poseduje nikakve podatke koji bi otkrili bilo šta što bi narušilo bezbednost sistema. Isto tako, napadač može da vrši i snimanje odgovora servera, koji sadrži u sebi jedinstveni identifikator privremenog tiketa i javni ključ vezan za taj identifikator. Ako napadač želi da ovo iskoristi na bilo koji način, ta mogućnost mu je veoma mala, jer je vreme trajanja privremenog tiketa za autentifikaciju veoma kratko. Pored toga, ako napadač želi da dešifruje odgovor klijenta serveru, koji je šifrovan sa javnim ključem servera, mora da dođe do privatnog ključa. Kako je praktično nemoguće (vremenski zahtevno) da se privatni ključ rekonstruiše iz javnog ključa, napadaču jedino preostaje da čeka da se privatni ključ na neki način kompromituje, da istekne digitalni sertifikat ili nešto slično..

Kada se izvrši uspešna autentifikacija i sva komunikacija između klijenta i servera za rad sa bazom podataka šifruje sa simetričnom kriptografijom, jedino što napadač može da izvrši je snimanje što više poruka i potom da pokuša da ih dešifruje potpunom pretragom po prostoru tajnih ključeva koji se koriste za šifrovanje i dešifrovanje. S obzirom, da se AES ključ i IV inicijalni vektor menjaju po svakoj uspešnoj autentifikaciji,

količina šifrata do koje napadač dolazi je veoma mala za uspešno dešifrovanje u realnom vremenu.

Implementacija ovih predloženih protokola rešenja za kriptografsku zaštitu memorije organizacije koja je bazirana na menadžmentu znanja, zasniva se i na trećoj strani od poverenja, odnosno servera za autentifikaciju. Pozitivna strana ovoga načina autentifikacije je da se postiže izvanredna bezbednost korisničkih kredencijala. Negativna strana je ukoliko server za autentifikaciju nije aktivan, čitav sistem je nepristupačan, jer usled nemogućnosti da se korisnik uspešno autentifikuje i dodeli tiket za rad sa serverom za rad sa bazom podataka memorije organizcaije ne može da se ostvari ni uspešna komunikacija.

Predloženo rešenje stavlja akcenat na zaštitu pristupa podacima od neovlašćenih lica. U rešenju nije razmatrana zaštita integriteta podataka od nemarnog ili zlonamernog delovanja lica koja imaju legitiman pristup podacima u memoriji organizacije. Takođe, nije razmatrana potreba za čuvanjem istorije svih promena nekog dokumenta ili grupe dokumenata na pouzdan način. Jedan od pravaca daljeg istraživanja bi mogao biti korišćenje *block-chain* strukture podataka za čuvanje čitave istorije promena dokumenata i garancijom da je takva struktura ispravna. tj. da nije bilo naknadnih izmena.

Takođe, korišćenje digitalnog potpisa garantuje da je dokument potpisan od strane autorizovanog lica, ali ne čuva prethodne verzije datog dokumenta unutar same kompanije. Na primer autorizovano lice može potpisati dokument u nekom trenutku vremena, zatim napraviti izmenu i ponovo ga potpisati čime se gubi informacija o sadržaju prethodne verzije tog potpisanog dokumenta. Formiranje *block-chain* strukture podataka u memoriji organizacije koja bi u svojim blokovima podataka sadržavala dokumenta, mogla bi da čuva istoruju svih dokumenata i kriptografski bi garantovala da istorija nije naknadno modifikovana.

Osnovni doprinosi ove disertacije pre svega odnose se na oblast kriptografskih rešenja zaštite memorije organizacije:

- U ovoj disertaciji se daje jedan novi generalizovan, model za zaštitu podataka, komunikacija, korišćenih kriptografskih ključeva, kontroli pristupa, čuvanju podataka, autentifikaciji i autorizaciji u jednoj kompaniji (organizaciji), koji omogućava rad u realnom vremenu, korišćenje podataka, a sve u cilju donošenja pravovremenih odluka.
- Predloženo rešenje kriptografske zaštite integrisanog automatizovanog sistema upravljanja memorije organizacije zasniva se na simetričnim i asimetričnim šifarskim sistemima i tehnologijama za pouzdano upravljanje kriptografskim ključevima (generisanje, distribucija, čuvanje, izbor, brisanje i sl.).
- Za realizaciju kriptografskih rešenja neophodno je koristite hardverske i softverske platforme i proizvode u koje se može imati poverenje (platforme otvorenog koda, proveriva hardverska osnova, bez tajnih vrata i sl.). U profesionalnim sistemima je dozvoljena upotreba samo sopstveno realizovanih kriptografskih algoritama (ne koriste se komercijalna rešenja), a sva kriptografska rešenja zaštite podataka treba da se zasnivaju na simetričnim šifarskim sistemima.
- Potpuna zaštita podataka se može ostvariti samo u izolovanim računarsko-komunikacionim sistemima, tj. sistemima koji su potpuno odvojeni od Internet mreže. Drugim rečima, ne postoji apsolutna zaštita kod realnih sistema koji su u

upotrebi. U kriptografiji se apsoluna zaštita vezuje samo za apsolutno tajne simetrične šifarske sisteme, a svi drugi sistemi koji su u upotrebi su praktično tajni, tj. računarski sigurni.

- Pored zaštite podataka neophodno je ostvariti potpunu kontrolu pristupa računarsko-komunikacionim resursima, zatim autorizaciju za rad pojedinih aplikacija, kvalitetnu autentifikaciju i sl. Svi pobrojani servisi se opet zasnivaju na kriptografskim rešenjima.
- Rešenje je zasnovano na upotebi korporativnih identifikacionih kartica u informacionom sistemu kompanije, pri čemu zaštitni mehanizmi obuhvataju višeslojnu arhitekturu zaštite (na aplikativnom, transportnom i mrežnom sloju), jake mehanizme kontrole pristupa kao i neke mehanizme zaštite baza podataka memorije organizacije kompanije koji otkrivaju i sprečavaju curenje podataka iz analitičkih sistema.
- Autentifikacija korisnika je dvo-faktorska. Klijent bez važećeg sertifikata smeštenog na pametnoj kartici nema prisup aplikaciji, a samim tim ni podacima u informacionom sistemu kompanije.
- Autorizacija korisnika je integrisana sa Aktivnim Direktorijumom, a administrativne dužnosti su podeljene na administraciju Aktivnog Direktorijuma i administraciju samog informacionog sistema kompanije.
- Šifrovanje podataka obavlja se hibridnim šifarskim sistemima, kojima se ostvaruju servisi tajnosti, integriteta, autentifikacije što se zasniva na digitalnim sertifikatima smeštenim na pametnim karticama.
- Curenje osetljivih podataka iz analitičkih sistema i baza podataka memorije organizacije sprečava se dodavanjem šuma u odgovor koji baza vraća korisniku, šifrovanjem podataka u transakcionim sistemima, onemogućavanjem određenog broja upita transakcionim sistemima spoljašnjim korisnicima i vođenjem dnevnika u kome je svaki zapis digitalno potpisan ključem koji se nalazi na pametnoj kartici.
- Pametne kartice se u predloženom rešenju štite PIN brojem.
- Krađa kartice i PIN broja može rezultovati digitalno potpisanim unosom u dnevničkoj datoteci koji korisnik ne može da opovrgne. U tom smislu se predlaže upotreba biometrije (na primer, otiska prsta, iris oka i sl.) u dvo-faktorskoj autentifikaciji umesto upotrebe PIN-broja, čime se sprečava moguća zloupotreba kartica u slučaju krađe i kompromitovanja PIN broja.

Ukoliko se predloženi sistem kritički analizira, mogu se uočiti i negativne strane ovakvih rešenja.

- Pre svega, rešenja mogu biti nepraktična i komplikovana za upotrebu. Kod takvih rešenja odziv sistema može biti veoma spor. Ukoliko se šifruju svi podaci i sve komunikacije, kao i pristup i kontrola resursima organizacije, upotreba takvih sistema je veoma složena, teška i sigurno vema spora. Dakle, primenom maksimalne kriptografske zaštite u svim segmentima u radu jedne organizacije dovodi do usporavanja i do neefikasnosti u komunikacijama.
- Kod složenih rešenja postoji veća mogućnost da se pogreši u radu, postoji više tačaka u kojima može doći do kompromitacije podataka. Protokoli za rad su takođe komplikovaniji i podložni su različitim hakerskim napadima na sam

protokol. Poseban problem kod takvih rešenja jeste ljudski faktor. Pokazuje se da sva složena rešenja imaju najslabiju kariku upravo kod ljudskog faktora.

Može se diskutovati i kolika je upotrebna vrednost ovakvih rešenja. Kada su informacija od izuzetnog značaja one moraju da se štite. Upravo je stvar kod upravljanja ovakvim sistemima, pa i kod projektovanja i realizacije, da se odredi prava mera potrebnih kriptografskih rešenja, kompleksnosti nosećih tehnologija, potrebnoj dužini i veku važenja kriptografskih ključeva i sl.

Na osnovu prezentovanih istraživanja i na osnovu predloga rešenja za projektovanje, realizaciju i eksploataciju izvodi se nekoliko suštinskih zaključaka. Korišćenjem integrisanog automatizovanog procesa upravljanja memorijom organizacije ostvaruje se politika sigurnosti, upravljanje i klasifikacija izvora, sigurnost zaposlenih, bezbednost materijalnih dobara i životne sredine, operativno upravljanje i komunikacija, kontrola pristupa, razvoj i održavanje sistema i upravljanje kontinuitetom poslovanja što doprinosi povećanju kvaliteta i efikasnosti poslovnog odlučivanja. Zaštitom integrisanog automatizovanog procesa upravljanja memorijom organizacije obezbeđuje se visok nivo sigurnosti i zaštite svih dokumenta kroz definisanje prava i ograničenja pristupa na nivou pojedinačnog korisnika ili grupa korisnika zajedno sa integrisanim programom za manipulaciju podacima u memoriji.

Shodno uočenim ograničenjima, smernice za dalji rad koji bi mogao da se nastavi u sklopu daljih istraživanja pre svega mogao bi da se odnosi na činjenicu da:

- Predloženo rešenje treba generalizovati, odnosno ponuditi radni okvir pogodan za implementaciju za sve operativne sisteme u praksi.
- Ovim načinom otvara se i mogućnost iskorišćavanja rešenja otvorenog koda čime bi se značajno doprinelo smanjenju troškova licenciranja (naročito za serversku familiju *Microsoft* operativnih sistema).

Literatura

[1] D. Kiron, R. Shockley, N. Kruschwitz, G. Finch, and M. Haydock, „Analytics: the Widening Divide, How companies are achieving competitive advantage through analytics.," *MIT Sloan Management Review with IBM Institute for Business Value*, 2011.

[2] J. Galbraith, „Organization Design Challenges Resulting From Big Data," *Journal of Organization Design*, no. 3(1), pp. 2-13, 2014.

[3] J. Galbraith, *Designing Organizations: Strategy, Structure, and Process at the Business Unit and Enterprise Levels*. San Francisco: Jossey Bass, 2014.

[4] R. Daft, *Organization Theory and Design (12th ed)*.: Cengage Learning, 2016.

[5] T. H., Davenport and L. Prusak, , *Working knowledge: How Organizations Manage What They Know*. Boston: Harvard Business School Press, 2000.

[6] K. Koskinen and P. Pihlanto, *Knowledge Management in Project-based Companies: An organic perspective*.: Palgrave Macmillan, 2008.

[7] J. Saaristo, *Knowledge management and sharing in multicultural SME companies. Case: Zilot International Ltd, Bachelor's Thesis*., 2012.

[8] R. Burton and B. Obel, *Strategic Organizational Diagnosis and Design, The Dynamics of Fit, Third Edition*.: Springer, 2004.

[9] T. H., Davenport, J. G. Harris, and R. Morison, *Analytics at Work: Smarter Decisions, Better Results*. Boston: Harvard Business Press, 2010.

[10] D. Klein, P. Tran-Gia, and M. Hartmann, „Big Data," *Informatik Spektrum*, no. 3, August 2013.

[11] J. Wetherbe and G. Browne, *Recognizing the Funcionality of the Future*, Competing in the Information Age, align in the sand ed., J. Luftman, Ed. Oxford University Press: Oxford:, 2003.

[12] D. Feeny, B. Ives, and G. Piccoli, *Creating and Sustaining IT-Enabled Competitive Advantage*, Competing in the Information Age, align in the sand ed., J. Luftman, Ed. Oxford: Oxford University Press, 2003.

[13] R. Hillard, *Information Driven Business: How to Manage Data and Information for Maximum Advantage*. New Jersey: John Wiley & Sons, 2010.

[14] Z. Glušica, *Menadžment znanja i menadžment kvaliteta u zborniku radova: Menadžment znanja*. Beograd: Univerzitet Braća Karić, Fakultet za menadžment, 2004.

[15] R. L. Ackoff, „From data to wisdom," *Journal of Applied Systems Analysis*, no. 15, pp. 3-9, 1989.

[16] J. Rowley, „The wisdom hierarchy: representations of the DIKW hierarchy.," *Journal of Information Science*, no. 33(2), pp. 163-180, 2007.

[17] D. Chaffey and S. Wood, *Business Information Management: Improving Performance Using Information Systems*. Harlow: FT Prentice Hall., 2005.

[18] A. Liew, „DIKIW: Data, Information, Knowledge, Intelligence, Wisdom and their Interrelationships," *Business Management Dynamics*, no. 2(10), pp. 49-62, 2013.

[19] C. Mader and R. Hagin, *Information Systems: Technology, Economics, Applications*.: Pearson Edication Ltd., 1979.

[20] R. Mason and U. Apte, „Using Knowledge to Transform Enterprises," in *Transforming Enterprise, The Economic and Social Implications of Information Technology*. Cambridge: The MIT Press., 2005, pp. 131-154.

[21] C. Williams, *Principi menadžmenta – MGMT*. Beograd: Data status, 2010.

[22] S. Nobre, A. Tobias, and D. Walker, „A New Contingency View of the Organization: Mananging Complexity and Uncertainnty Trough Cognition," *Brazilian Administration Review*, vol. VII, no. 4, pp. 379-396, December 2010.

[23] S. McShane and M. Von Glinow, *Organizational Behavior*.: McGraw-Hill Education, 2009.

[24] S. Kudyba and M. Kwatinetz, „Introduction to the Big Data Era," in *Big Data, Mining, and Analytics*.: CRC Press, Taylor & Francis Group, 2014, pp. 1-17.

[25] E. Turban, E. McLean, and J. Wetherbe, *Informaciona tehnologija za menadžment, transformisanje poslovanja u digitalnu ekonomiju,* Beograd: Zavod za udžbenike i nastavna sredstva, 2003.

[26] D. Spitzer, *Transforming Performance Measurement: Rethinking the Way We Measure and Drive Organizational Success*. New York: American Management Association, 2007.

[27] D. Foray, „New Models of Innovation and the Role of Information Technologies in the Knowledge Economy," in *Transforming Enterprise, The Economic and Social Implications of Information Technology*. Cambridge: The MIT Press, 2005, pp. 113-129.

[28] J. Albus, „Outline for a Theory of Intelligence," *IEEE Transactions on Systems, Man, and Cybernetics*, pp. 473-509, 1991.

[29] E. Awad and H. Ghaziri, *Knowledge Management*, Pearson Education International, Ed. New Jersey, 2004.

[30] R. Sternberg, „Implicit theories of intelligence, creativity, and wisdom," *Journal of Personality and Social Psychology,* pp. 607-627, 1985.

[31] G. Bellinger. (2004) Knowledge Management-Emerging Perspectives. Document. [Online]. http://www.systems-thinking.org/kmgmt/kmgmt.htm#dac

[32] M. Zack, „Developing a Knowledge Strategy," *California Management Review*, vol. XLI, no. 3, 1999.

[33] B. Meyer and K. Sugiyama, „The concept of knowledge in KM: a dimensional model," *Journal of Knowledge Management*, no. 11(1), pp. 17-35, 2007.

[34] S. Kermally, *Effective knowledge management*. West Sussex: John Wiley & Sons, 2002.

[35] K.E. Sveiby, *The New Organizational Eealth: Managing and Measuring Knowledge-Based Assets*.: Berrett-Koehler Publishers, Inc., 1997.

[36] Van J. Beveren, „A model of knowledge acquisition that refocuses knowledge management," *Journal of Knowledge Management*, no. 6(1), pp. 18-22, 2002.

[37] R. McDermott, „Why information technology inspired but canot deliver knowledge management," *California Management Review*, no. 41(4), pp. 103-117, 1999.

[38] M. Alavi and D. E. Leidner, „Review: Knowledge management and knowledge management systems: conceptual foundations and research issues," *MIS Quarterly*, no. 25(1), pp. 107-136, 2001.

[39] R. C. Hicks, R. Dattero, and S. D. Galup, „The five-tier knowledge management hierarchy," *Journal of Knowledge Management*, no. 10(1), pp. 19-31, 2006.

[40] C. C. Lee and J. Yang, „Knowledge value chain," *Journal of Management Development,* no. 19 (9), pp. 783-793.

[41] C.M. Rumizen, *The Complete Idiot's Guide To Knowledge Management*. Indianapolis: Alpha Books, 2002.

[42] I. Nonanka, R. Toyama, and N. Konno, „A Unified Model of Dynamic Knowledge Creation Long Range Plannig," *SECI, Ba and Leadership*, vol. XXXIII, no. 1, pp. 5-34, February 2000.

[43] A. C. Edmondson, B. Winslow, M. Bohmer, and P. Pisano, „Learning how and learning what: effects of tacit and codified knowledge on performance improvement following technology adoption," *Decision Sciences*, no. 34 (2), pp. 197-223, 2003.

[44] N. Mooradian, „Tacit knowledge: pholosophic roots and role in KM," *Journal of Knowledge Management*, no. 9 (6), pp. 104-113, 2006.

[45] P. Murray, „Information, knowledge and document management technology," *KM Briefs and KM Magazine*, 2000.

[46] I. Nonaka and H. Takeuchi, *The Knowledge Creating Company*. New York: Oxford University Press, 1995.

[47] J. Đorđević Boljanović, *Menadžment znanja*: Data status, 2009.

[48] M. Tsai and K. Lee, „A study of knowledge internalization: from the perspective of learning cycle theory," *Journal of Knowledge Management*, no. 10(3), pp. 57-71.

[49] C. Hicks, R. Dattero, and D. Galup, „The five-tier knowledge management hierarchy," *Journal of Knowledge Management,* no. 10 (1), pp. 19-31, 2006.

[50] B. Vukšić, *Upravljanje znanjem*. Zagreb: Ekonomski fakultet, 2000.

[51] M. Thomas, S. Koulopoulos, and W. Toms, *Corporate Instinct: Building a Knowing Enterprise for the 21st Century*.: Wiley, 1997.

[52] B. Krstić, „Objectives, Types, and Efficiency Factors of Knowledge Management Projects," in *Upravljanje projektima – nove tendencije*, Zlatibor, 2001, pp. 324-328.

[53] C Frappaoli, *Knowledge management*: Capstone Publishing Ltd., Wiley, 2006.

[54] B. Krstić and V. Sekulić, *Upravljanje performansama preduzeća*, Niš: Ekonomski fakultet, 2013.

[55] J. DiBella and C. Nevis, *How organizations learn: an integrated*. San Francisco: Jossey-Bass, 1998.

[56] M. Jensen and F. Luthans, „Entrepreneurs as authentic leaders: Impact on employees' attitudes," *Leadership and Organization*, no. 27(8), pp. 646-666, 2006.

[57] M. Chen and A. Chen, „Knowledge management performance evaluation: a decade review from 1995 to 2004," *Journal of Information Science*, no. 32(17), pp. 17-38, February 2006.

[58] D. Day and C. Wendler, „Best Practice and Beyond: Knowledge Strategies," *McKinsey Quarterly Winter edition*, 1998.

[59] M. Mazur et al., *Upravljanje znanjem 2.0: Priručnik za poduzeća.*: Lifelong Learning Programme, 2014.

[60] B. Mierzejewska and D. Shaver, „Key Changes Impacting Media Management Research," *The International Journal on Media Management*, vol. XVI, no. 2, 2014.

[61] G. Probs, K. Raub, and K. Romhard, *Managing Knowledge: Building Blocks for Success.*: Wiley, 1999.

[62] V. Kotlenikov. (2015) New Economy: Key Features of the New Rapidly Globalizing and Changing Knowledge Economy. [Online]. http://www.1000ventures.com

[63] R. Tisen, D. Andriessen, and L. Depre, *Dividenda znanja*. Novi Sad: Adžies, 2006.

[64] N. Valaei and A. Aziz, „Awareness: A Study of Knowledge Management Adoption amongst Iranian SMEs," *Journal of Organizational Knowledge Management*, 2012.

[65] A. Hylton, *Measuring & Assessing Knowledge-Value & the Pivotal Role of the Knowledge Audit.*: Hylton Associates, 2002.

[66] C. Lee, C. Egbu, D. Boyd, H. Xiao, and E. Chinyo, „Knowledge Management for Small Medium Enterprise: Capturing and Communicating Learning and Experiences," in *4th Triennial International Conference Rethinking and Revitalizing Construction Safety, Health, Environment and Quality*, 2005, pp. 808-820.

[67] C. Egbu, „Knowledge Management and HRM: The role of the Project Manager.," in *PMI Europe 2001 – A Project Management Odyssey*, 2001.

[68] R. Rothwell and M. Dodgson, *Innovation and size of firm, The handbook of industrial innovation.*, 1994.

[69] G. Krogh, K. Ichijo, and I. Nonaka, *Enabling Knowledge Creation: How to Unlock the Mystery of Tacit Knowledge and Release the Power of Innovation.*, 2000.

[70] R. McAdam and R. Reid, „SMEs and Large Organisation Perceptions of Knowledge Management: Comparisons and Contrasts," *Journal of Knowledge Management*, no. 5(3), pp. 231-241, 2001.

[71] A. Paarup Nielsen, „Understanding dynamic capabilities through knowledge management," *Journal of Knowledge Management*, no. 10 (4), pp. 59-71, 2006.

[72] P. Beijerse, „Knowledge management in small and medium-sized companies: knowledge management for entrepreneurs," *Journal of Knowledge Management*, no. 4(2), pp. 162–179, 2000.

[73] M. Corso, A. Martini, E. Paolucci, and L. Pellegrini, „Knowledge management in product innovation: an interpretative review," *International Journal of Management Reviews*, no. 3(4), pp. 341–352, 2001.

[74] R. Edvardsson, „Knowledge management in SMEs: the case of Icelandic firms", *Knowledge Management Research & Practice*, no. 4, pp. 275-282, 2006.

[75] S. Salojärvi, P. Furu, and E. Sveiby, „Knowledge management and growth in Finnish SMEs," *Journal of Knowledge Management*, no. 9, pp. 103-122, 2005.

[76] C. O'Dell et al., *Successfull KM implementations: A study of best practice organizations, Handbook on knowledge management*.: Springer, 2009.

[77] M. Wunram, F. Weber, K. Pawar, A. Horton, and A. Gupta, „Proposition of a Humancentered Solution Framework for KM in the Concurrent Enterprise," in *International Conference on Concurrent Enterprising*, 2002.

[78] J. Crager and D. Lemons, *Measuring the Impact of Knowledge Management*.: American Productivity and Quality Center, 2003.

[79] D. Streatfield and D. Wilson, „Deconstructing knowledge management," *Aslib Proceedings*, no. 51, pp. 67-71, 1999.

[80] S. Seiner, „Knowledge Management: It's Not All About the Portal," *The Data Administration Newsletter*., 2001.

[81] M. Levinson, „Knowledge Management Definition and Solutions," *CIO Magazin*, 2007.

[82] E. Sveiby, „What is Knowledge Management?," *Journal of Knowledge Management*, no. 9(2), pp. 103-122, 2005.

[83] R. Villegas, *Knowledge Management White Paper*.: KMPeer Publishing, 2002.

[84] Estacio, *Benefits and challenges of knowledge management*.: WLE, 2006.

[85] P. Murray and A. Myers, „The facts about knowledge," *Information Strategy*, pp. 31-33, September 1997.

[86] Y. Malhotra, „Knowledge Management and New Organization Forms: A Framework for Business Model Innovation," *Information Resources Management Journal*, no. 13(1), pp. 5-14, January-March 2000.

[87] D. Skyrme, *Knowledge Management: Approaches and Policies*, David Skyrme Associates Limited, Ed.: Higclere, 2006.

[88] W. Bock and J. Senne, *Cyber Power for Business: How to profit from the information superhighway*.: Career Press, 1996.

[89] [Online]. http://www.knowledgepoint.com.au

[90] M. Alavi and E. Leidner, „Knowledge Management Systems: Issues, Challenges, and Benefits, Communications of the AIS," in *A Framework of Knowledge Management Systems: Issues and Challenges for Theory and Practice*, 21st International Conference on Information Systems, Ed. Brisbane, Australia: Carlson School of Management, University of Minnesota, 2000, ch. 7.

[91] H. Koontz, H. Weihrich, and S. Freeman, *Preinciples of management*.: Rai Technology University, 2013.

[92] D. Vera and M. Crossan, „Organizational Learning and Knowledge Management: Toward an Integrative Framework," in *The Blackwell Handbook of Organizational Learning and Knowledge Management*. Oxford: Blackwell Publishing, 2005, pp. 122-142.

[93] J. Riderstrale and K. Nordstrom, *Funky Business*, Beograd: Plato, 2002.

[94] A. Mayo, „The role of employee development in gowth of intellectual capital," *Personal Review*, p. 524, 2000.

[95] D. Đuričin and S. Janošević, *Strategijska analiza ljudskih resursa*, Niš: Ekonomski fakultet Niš, 2009.

[96] E Sveiby and T. Llayd, *Managing Know-how. By Valuing Creativity*. London: Blomsbury, 1987.

[97] A. Steven and K. Bradley, *The Management if Intellectual Capital*. London: The Business Performanse Group Limited, 1995.

[98] V. Srića and M. Spremić, *Informacijskom tehnologijom do poslovnog uspjeha*, Zagreb: Sinergija, 2000.

[99] M. Spremić, „Znanje i intelektualni kapital – skrivena vrijednost kompanije", *Računovodstvo i financije*, no. 8, p. 17, 2001.

[100] R. Petty and J. Guthrie, „The Case for Reporting an Intellectual Capital: Evidence, Analysis and Future Trends," in *The Current State of the Business Discipline*. Rohtak: Spellbound Publications, p. 19.

[101] ICDQM, *Zbornik radova – Upravljanje kvalitetom i pouzdanošću*, Čačak: Izdavački centar DQM, 2008.

[102] N. Pavlović, *Osnovi organizacije,* Novi Sad: Alga – Graf NS, 2007.

[103] Č. Ljubojević, *Marketing usluga*,Novi Sad: Stilos, 2002.

[104] L. Edvinsson, *Korporacijska longituda – Navigacija ekonomijom znanja*, Zagreb: Differo, 2003.

[105] B. Garvey and B. Willianson, *Beyond Knowledge Management*.: Pearson Education, Ltd., 2002.

[106] A. Stewart, *The Intellectual Capital, the New Wealth of Organization*. New York: Doubleday, 1997.

[107] K.E. Sveiby, *The New Organizational Wealth: Managing and Measuring*. San Francisco: Berrett Koehler, 1997.

[108] G. Dess, T. Lumpkin, and A. Eisner, *Strategijski menadžment,* treće izdanje, Beograd: Data status, 2007.

[109] R. Ruggles, *Knowledge Management Tools*.: Taylor and Francis, 2011.

[110] Gotcha. (1999) Berkeley.edu. [Online]. http://www.sims.berkeley.edu/courses/is213/s99/Projects/P9/web_site/index.html

[111] B. Krstić and D. Vukadinović, „Upravljanje znanjem kao izvor održive konkurentnosti preduzeća", *Ekonomske teme*, no. 3, p. 90.

[112] R. Tisen, D. Andriesen, and F. Lekan Depre, *Dividenda znanja – stvaranje kompanija sa visokim učinkom kroz upravljanje znanjem kao vrednošću*, Beograd: HESPERIA EDU, 2006.

[113] B. Komnenić, *Vrednost vs profit – Koncept intelektualnog kapitala*, Beograd: Zavod za udžbenike, 2013.

[114] K. Dalkir, *Knowledge management in Theory and Practice*.: Elsevier, 2005.

[115] J. Lebowitz, *Knowledge management Handbook*. Washington DC: CRC Press, 1999.

[116] M. Beer, B. Spector , P. R. Lawrence, D. Q. Mills, and R. E. Walton, *Managing Human Assets*. New York: The Free Press, 1984.

[117] K. M. Wiig, *Knowledge Management Foundations: Thinking about Thinking – How people and Organisations Create, Represent, and Use Knowledge*. Arlington: Shema Press, 1993.

[118] G. Von Krogh and J. Roos, *Organizational epistemology*.: St. Martin's Press, 1995.

[119] M. H. Boisot, *Knowledge assets: Securing competitive advantage in the information economy*. New York: Oxford University Press, 1998.

[120] C. W. Choo, *The knowing organization: How organizations use information to construct meaning, create knowledge, and make decisions*. New York: Oxford University Press, 1998.

[121] D. Bennet and A. Bennet, „The depth of KNOWLEDGE: Surface, shallow and deep in VINE," *Journal of information and knowledge management systems*, no. 38(4), pp. 405-420, 2008.

[122] K. M. Wiig, *Knowledge management Methods: Practical Approaches to managing Knowledge*. Arlington: Shema Press, 1995.

[123] K. M. Wiig, *Knowledge Management, The Central Management Focus for Intelligent-Acting Organizations*. Arlington: Shema Press, 1994.

[124] K. M. Wiig, R. De Hoog, and R. Van der Spek, „Supporting Knowledge Management: A Selection of Methods and Techniques," *Expert Systems With Applications*, no. 13(1), pp. 15-27, 1997.

[125] Ž. Adamović, *Upravljanje proizvodom.* Srpsko Sarajevo: Zavod za udžbenike, 2002.

[126] Ch. Collison and G. Parcell, *Learning to fly: Practical knowledge management from some of the world's leading organizations*. Capstone: Chichester, 2004.

[127] J. Karlsen and P. Gottschalk, „Factors Affecting Knowledge Transfer in IT Projects," *Engineering Management Journal*, no. 16(1), 2004.

[128] P. Gottschalk, *Strategic Knowledge Management Technology*. London : Idea Group Publishing, 2005.

[129] V. Hlupic, *Knowledge and Business Process Management*.: IDEA Group Publishing, 2003.

[130] N. Wickramasinghe and D. Von Lubitz, *Knowledge – Based Enterprise: Theories and Fundamenta*. London: Idea Group Publishing, 2007.

[131] S. Franklin and A. Graesser, *Is it an Agent, or just a Program? A Taxonomy for Autonomous Agents*.: Institute for Intelligent Systems, University of Memphis, 1996.

[132] N. Balaban and Ž. Ristić, *Poslovna inteligencija*, Subotica: Ekonomski fakultet, 2006.

[133] M. Hammer and J. Champy, *Reengineering the corporation*. New York: Harper Collins, 1994.

[134] H. Johansson, P. McHugh, J. Pendlebury, and W. Wheeler, *Busines process reengineering: breakpoint strategies for market dominance*, New York: Wiley&Sons Ltd., 1994.

[135] V. Srića, *Menadžerska informatika*, Zagreb: M.E.P. Consult, 1999.

[136] Lj. Trifunović and B. Stavrić, *Poslovna organizacija*, Univerzitet u Istočnom Sarajevu, Ekonomski fakultet Brčko, 2010.

[137] P. Sikavica and M. Novak, *Poslovna organizacija,* Zagreb: Informator, 1999.

[138] A. Majchrzak and Q. Wang, „Breaking the functional mind-set in process organizations," *Harvard Business Review*, 1996,pp. 93-99.

[139] F. Ostroff, *The Horizontal Organization*.: Oxford University Press, 1999.

[140] J. Power, *Decision Support Systems: Concepts and Resources*. Cedar Falls: IA: DSS, 2000.

[141] M. Čupic, R. Tummala, and M. Suknović, *Odlučivanje – formalni pristup*, Beograd: Fakultet organizacionih nauka, 2001.

[142] D. Bečejski Vujaklija, „Metodološke osnove ekspertskog ocenjivanja u funkciji podrške odlučivanju", in *SIMORG 91*, Kopaonik, 1991, pp. 158-165.

[143] E. Turban, *Decision Support and Expert Systems*. London: Mackmilan Publishing Company, 1988.

[144] E. Turban, *Decision Support, Expert Systems: Management Support Systems, 4th edition*. New York: Prentice Hall, 1995.

[145] E. Turban, E. McLean, and J. Wetherbe, *Information Technology for Management*. New York: John Wiley & Sons, Inc., 1996.

[146] E. Turban, J. Aronson, and T-P. Liang, *Decision Support Systems and Intelligent Systems (7th Edition)*. New York: John Wiley & Sons, Inc., 2005.

[147] G. Klepac, *Primjena inteligentnih računalnih metoda u managementu*, Zagreb: Sinergija, 2001.

[148] R. Sprague and H. Watson, *Decision Support Systems – putting theory into practice*. London-Sydney-Toronto: Prentice Hall, 1989.

[149] S. Alter, „A work system view of DSS in its fourth decade", *Decision Support Systems*, no. 38(3), pp. 319-327, 2004.

[150] A. Veljović, M. Radojičić, and J. Vasić, *Menadžment informacioni sistemi*, Čačak: Tehnički fakultet, 2008.

[151] A. E. Feigenbaum, *The Rise of the Expert Company: How Visionary Companies Are Using Artificial Intelligence to Achive Higher Productivity and Profits*. Vintage: Crown Publishing Group, 1990.

[152] M. Suknović, *Poslovna inteligencija i sistemi za podršku u odlučivanju,* Beograd: Fakultet organizacionih nauka, 2010.

[153] V. M. Ribière, *Assessing Knowledge Management Initiatives' Success as a Function of Organizational Culture*. Washington D.C.: The School of Engineering Management and Systems Engineering, The George Washington University, 2001.

[154] S. Milovanović, „Informacioni sistemi za kreiranje znanja u preduzeću", in *VII Skup privrednika i naučnika – SPIN´09 Operacioni Menadžment i globalna kriza*, Beograd, 2009, pp. 626-632.

[155] J. Swart and N. Kinnie, „Sharing Knowledge in Knowledge-intensive Firms," *Human Resource Management Journal*, no. 3(2), pp. 60–75, 2003.

[156] K. O'Sullivan, „Leveraging Knowledge Management Technologies to Manage Intellectual Capital," in *Creating the Discipline of Knowledge Management – The Latest in University Research*. Amsterdam: Elsevier Butterworth–Heinemann, 2005, pp. 134-140.

[157] L. Edvinsson and S. Malone, *Intellectual Capital: Realizing Zour Company's TRue Value by Finding Its Hidden Brainpower*. New York: HarperCollins Publishers, Inc., 1997.

[158] D. Harris, *Organisational Management and Information Systems, CIMA Exam Practice kit*.: Elsevier, Ltd., 2007.

[159] D. Sparkes, *Organisational Management and Information Systems, CIMA Exam Practice kit*.: Elsevier, Ltd., 2008.

[160] P. Senge, *The fifth discipline: the art and practice of the learning organization*. Novi Sad: Adižes, 2003.

[161] M. Dierkes, A. Berthoin Antal, J. Child, and I. Nonaka, *Handbook of Organizational Knowledge*.: Oxford University Press, 2001.

[162] S. F. Slater and J. C. Narver, „Market orientation and learning organization," *Journal of Marketing*, no. 59, pp. 63-74, 1995.

[163] A. D. Ellinger, A. E. Ellinger, B. Yang, and S. W. Howton, „The relationship between the learning organization concept and firms' financial performance: an empirical assessment," *Human Resource Development Quarterly*, no. 13(1), pp. 5-21, 2002.

[164] V. J. Marsick and K. E. Watkins, *Facilitating learning organizations: Making learning count*. Aldershot: Gower, 1999.

[165] J. Peters, „A learning organization syllabus," *Learning Organization*, no. 3(1), pp. 4-10, 1996.

[166] D. Robey, M.C. Boudreau, and G.M. Rose, „Information technology and organizational learning: a review and assessment of research," *Accounting, Management and Information Technologies*, no. 10, pp. 125-155, 2000.

[167] K. E. Watkins and V. J. Marsick, *Sculpting the learning organization: Lessons in the art and science of systemic change*. San Francisco: Jossey-Bass, 1993.

[168] K. E. Watkins and V. J. Marsick, *In action: Creating the learning organization*. Alexandria: VA: American Society for Training and Development, 1996.

[169] D. A. Garvin, „Building a learning organization," *Harvard Business Review*, no. 71(4), pp. 78-88, 1993.

[170] M. Marquardt, *Building the learning organization: mastering the five elements for corporate learning*. Palo Alto: CA: Davies-Black Publishing, 2002.

[171] R. Kimball and M. Ross, *The Data Warehouse Toolkit: The Complete Guide to Dimensional Modeling, 2nd Edition*.: Wiley, 2002.

[172] B. Larson, *Delivering Business Intelligence with MS SQL Server 2008*.: Mc Graw Hill, 2009.

[173] D. Barry, *Data Warehouse from Architecture to Implementation*.: Addison-Wesley, 1997.

[174] V. Rainardi, *Building a Data Warehouse: With Examples in SQL Server*.: Apress, 2008.

[175] A. Njeguš, *Poslovni informacioni sistemi*, Beograd: Singidunum, 2008.

[176] D. Krneta and D. Radosav, „Realization Business Intelligence system using MS SQL Server 2008", in *FIT IT Conference*, Mostar, 2008.

[177] V. Milićević, *Internet ekonomija,* Beograd: Fakultet organizacionih nauka, 2002.

[178] G. Klepac and Ž. Panian, *Poslovna inteligencija*, Zagreb: Masmedija, 2003.

[179] Ž. Panian, *Poslovna inteligencija – Studije slučajeva iz hrvatske prakse*, Zagreb: Narodne novine d.d., 2007.

[180] D. Leffingwell and D. Muirhead, *Tactical Management of Agile Development: Achieving Competitive Advantage*.: Rally Software Development Corporation, 2004.

[181] H. D. Morris, R. Blumstein, and D. Vesset, „SAP's Business Analytics Solution: Applying Intelligence to Drive Value Through the Enterprise," in *Handbook on Decision Support Systems 2*.: Springer, 2008.

[182] D. E. Sharp, *Customer Relationship Management Systems Handbook*. Boca Raton: Auerbach Publications, 2002.

[183] I. H. Witten, F. Eibe, and M. A. Hall, *Data Mining: practical machine learning tools and techniques*. USA: Morgan Kaufmann, 2011.

[184] Pang N. T., M. Steinbach, and V. Kumar, *Introduction to Data Mining*.: Pearson Addison Wesley, 2005.

[185] J. D. Hand, H. Mannila, and P. Smyth, *Princeples of Data Mining*.: MIT press, 2001.

[186] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning, Data Mining, Inference, and Prediction*.: Springer, 2008.

[187] K. A. Pujari, *Data Mining Techniques*. India: Universities Press, 2001.

[188] S. Tuffery, *Data Mining and Statistics for Decision Making*.: Wiley, 2011.

[189] C. C. Aggarwal, *Data Mining, The Textbook*.: Springer, 2015.

[190] G. Williams, *Data Minig with Rattle and R, The art of Excavating Data for Knowledge Discovery*.: Springer, 2012.

[191] I. D. Olson and D. Delen, *Advanced Data Mining Techniques*.: Springer, 2008.

[192] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, „From Data Minig to Knowledge Discovery in Databases", *Al Magazine*, vol. XVII, no. 3, 1996.

[193] B. Delibašić, M. Suknović, and M. Jovanović, *Algoritmi mašinskog učenja za otkrivanje zakonitosti u podacima*, Beograd: Fakultet organizacionih nauka, 2009.

[194] F. Buttle, *Customer Relationship Management*. Oxford: Elsevier, 2009.

[195] M. Kantardžić, *Data mining concepts, models, methods and algorothms*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2011.

[196] Z. Tang and J. MacLennan, *Data Mining with SQL Server 2005*. Indianapolis: Wiley Publishing Inc., 2005.

[197] C. Baragion et al., *Mining Your Own Business in Banking Using DB2 Intelligent Miner for Data*. San Jose, USA: IBM Redbook, 2001.

[198] D. Pyle, *Data Preparation for Data Mining*. San Franciso: Morgan Kaufmann, 1999.

[199] A. J. Scott and C. J. Wild, „Fitting Logistic Models under Case-control or Choice Based Sampling", *Journal of the Royal Statistical Society Series B*, no. 48(2), pp. 170-82, 1986.

[200] M. J. Berry and G. S. Linoff, *Mastering Data Mining*. Chichester: Wiley, 2000.

[201] S. Garcia, Luengo, Julian, and F. Herrera, *Data Processing in Data Mining*. London: Springer-Verlag, 2016.

[202] B. S. Appavau and C. A. B. Arockia , *Insight into Data Preprocessing: Theory and Practice, Data Mining Perspective*.: Lambert Academic Publishing, 2012.

[203] S. Chakrabarti et al., *Data Mining, Know It All*.: Elsevier, Morgan Kaufman Publishers, 2009.

[204] F. Liu and B. Shih, *Application of Data-Mining Technology on E-Learning Material Recommendation, E-learning Experiences and Future*.: InTech, 2010.

[205] C. Romero, S. Ventura, M. Pechenizkiy, and R.S. Baker, *Handbook of Educational Data Mining*. USA: CRC Press, 2010.

[206] M. Mehedy, K. Latifur, and T. Bhvani, *Data Mining Tools for Malware Detectio*.: CRC Press Taylor &Francis Group, 2011.

[207] Two Crows Corporation, *Introduction to Data Mining and Knowledge Discovery Third Edition*.: Two Crows Corporation, 1999.

[208] R. Dubes and A. K. Jain, „Clustering techniques: The user's dilemma ", *Pattern Recognit*, no. 8(4), pp. 247-258, 1976.

[209] J. R. Garambeier, *A Techniques of cluster algorithms in data mining*.: J Data Min Knowl Discovery, 2002.

[210] A. K. Jain, M. N. Murty, and P. J. Flynn, „Data clustering: A review", *ACM Computer Survey*, no. 31(3), pp. 264-323, 1999.

[211] B. Rama, P Jayashree, and S. Jiwani, „A survey on clustering. Current status and challenging issues", *International Journal on Computer Science and Engineering*, no. 2(9), pp. 2976-80, 2010.

[212] L. Rokach and O. Maimon, „Clustering methods," in *Data mining and knowledge discovery handbook*. New York: Springer Verlag, 2005, pp. 321-352.

[213] R. Xu and D. Wunsch , „Survey of clustering algorithms", *IEEE Trans Neural Network*, no. 16(3), pp. 645-678, 2005.

[214] M. Bramer, *British Library Cataloguing in Publication data*. London: Springer-Verlag London limited, 2007.

[215] Du. Ke-Lin and N. S. Swamy, *Neural Networks and Statistical Learning*. London: Springer-Verlag, 2014.

[216] I. A. Galushkin, *Neural Networks Theory*. Berlin: Springer-Verlag Berlin Heidelberg, 2007.

[217] L. Breiman, J. H. Friedman, R. A. Olshen, and C. J. Stone, *Classification and Regression Trees*. Wadsworth, 1984.

[218] J. R. Quinlan, *C4.5 Programs for Machine Learning*.: Morgan Kaufmann, 1993.

[219] Z. Cerović, *Hotelski menadžment*, Opatija: Fakultet za turistički i hotelski menadžment, 2003.

[220] A. E. Eiben, P. E. Raué, and Z. Ruttkay, „Genetic Algorithms with multi-parent recombination," in *Parallel Problem Solving from Nature*, Berlin, Heidelberg, New York: Springer, 1994, pp. 78-87.

[221] A. Menon, *Frontiers of Evolutionary Computation*.: Kluwer Academic Publishers, 2004.

[222] N. Žalac, „Rudarenje podataka i njihovo pretvaranje u znanje", *Hrvatska gospodarska revija*, no. 6, p. 96, 2000.

[223] E. K. Mohamed, E. F. Abdelaziz, and C. Ellis, „Enterprise workflow, corporate memory, and decision-making," in *Multimedia Computing and Systems (ICMCS), International Conference*, 2011, pp. 1-8.

[224] L. Zhang, L. Bao-Wei, and T. Ye-Zhuang, „Empirical Study on Organizational Memory Constructive Factors", in *Management Science and Engineering, ICMSE 2007. International Conferenc*, 2007, pp. 1487-1492.

[225] A. Strauss, *Creating Sociological Awareness: Collective Images and Symbolic Representations*. New Brunswick: Transaction, 1991.

[226] M. Alvarado, „Automatizacio´n de la Administracio´n del Conocimiento para Negocios Electro´nicos," in *Simposio Internacional de Sistemas de Informacio´n. SISTINF01*, Mexico, 2001.

[227] C. B. Garcia and H. C. Howard, „Acquiring design knowledge through design decision justification," *AL EDAM Journal*, no. 6, pp. 1-13, 1992.

[228] P. J. Walsh and G. R. Ungson, „Organization-memory," *Academy of Management Review*, no. 16(1), 1991.

[229] G. Van Heijst, R. Van Der Spek , and E. Kruizinga, „Corporate memories as a tool for knowledge management", *Expert systems with applications*, no. 13(1), pp. 41-54, 1997.

[230] C. C. Huang, Y. N. Fan, C. C. Chern, and P. H. Yen, „Measurement of analytical knowledge-based corporate memory and its application", *Decision Support Systems*, no. 54(2), pp. 846-857, 2013.

[231] Euzenat, „Corporate memory through cooperative creation of knowledge bases and hyper-documents", in *10th workshop on knowledge acquisition (KAW)*, Banff (CA), 1996, pp. 1-18.

[232] M. Nagendra Prasad and E. Plaza, „Corporate Memories as Distributed Case Libraries," in *KAW'96*, Banff, Alberta, Canada, 1996, pp. 40-1- 40-19.

[233] F. Pomian, *Mémoire d'entreprise, techniques et outils de la gestion du savoir.*: Ed Sapienti, 1996.

[234] H. Simon, *The Sciences of the Artificial*, 3rd ed.: MIT Press, 1996.

[235] M. Grunstein, *La capitalisation des connaissances de l'entreprise, système de production de connaissances.*: Aix-en-Provence, 1995.

[236] J. Chosnek, „Maintaining the corporate memory," *Journal of Loss Prevention in the Process Industries*, no. 23, pp. 796-798, 2010.

[237] Y. Jussupova-Mariethoz and A.R. Probst, „Business concepts ontology for an enterprise performance and competences monitoring," *Computers in Industry*, no. 58(2), pp. 118-129, 2007.

[238] E. W. Stein and V. Zwass, „Actualizing organizational memory with information systems," *Information systems research*, no. 6(2), pp. 85-117, 1995.

[239] C. C. Huang, T. L. B. Tseng, and A. Kusiak, „XML-based modeling of corporate memory. Systems, Man and Cybernetics, Part A: Systems and Humans," *IEEE Transactions*, no. 35(5), pp. 629-640, 2005.

[240] I. Azbel and S. Berman, „An Epistemic Model as the Basis for a Corporate Memory," in *13th international conference on application of Prolog (INAP),* Tokyo, Japan , 2000, pp. 71-76.

[241] A. Verma, M.K. Tiwari, and N. Mishra, „Minimizing time risk in on-line bidding: An adaptive information retrieval based approach," *Expert Systems with Applications*, no. 38(4), pp. 3679-3689, 2011.

[242] W. Ceusters and B. Smith, *Referent Tracking for Corporate Memories, Handbook of Ontologies for Business Interaction*. New York, London: Idea Group Publishing, 2007.

[243] M. R. Mendenhall, „Corporate memory contribution to integrated design and analysis systems," *Aeronautical Journal,* no. 110(1106), pp. 257-263, 2006.

[244] O. Kühn and A. Abecker, „Corporate memories for knowledge management in industrial practice: Prospects and challenges", in *Information technology for knowledge management*. Berlin: Springer Berlin Heidelberg, 1998, pp. 183-206.

[245] M. Grunstein and J. P. Barthès, „An Industrial View of the Process of Capitalizing Knowledge", in *Knowledge Management: Organization, Competence and Methodology*. Rotterdam, Netherlands: Ergon Verlag, 1996, pp. 258-26.

[246] M. Durstewitz. (1994) Report on Workshop on Corporate Memory. Document. [Online]. http://www.delab.sintef.no/MNEMOS/external-info/cm-eurisko.txt

[247] T. V. Van Engers, H. Mathies, J. Leget, and C. C. Dekker, „Knowledge Management in the Dutch Tax and Customs Administration: Professionalisation within a Knowledge Intensive Organization," in *ISMICK'95*, Compiègne, 1995, pp. 71-80.

[248] R. Dieng et al., „Building of a Corporate Memory for Traffic Accident Analysis," *AI Magazine*, no. 19, 1998.

[249] R. Chakhmoune, H. Behja, and A. Marzak, „Building corporate memories in collaborative way using ontologies – Case study of a SSII," in *3rd International Conference on Next Generation Networks and Services*, 2011.

[250] P. A. Tourtier, *Analyse préliminaire des métiers et de leurs interactions. Rapport intermédiaire du projet GENIE.*: INRIA-Dassault-Aviation, 1995.

[251] P. Thomas, *Introduction: CSCW Requirements and Evaluation*. London: Springer, 1996.

[252] S. Buckingham Shum, „Negotiating the construction and reconstruction of organisational memories," *Journal of Universal Computer Science,* no. 3(8), pp. 899-928, 1997.

[253] C. Guérin and T. Mahé, „Entreprises, exercez votre mémoire!," *Sciences et Techniques,* no. 784, 1997.

[254] T. Kurland and P. Barber, „User requirements from a group perspective: the case of distance learning mediated by computer conferencing," in *CSCW Requirements and Evaluation*. London: Springer, 1995, pp. 57-74.

[255] S. Jones and S. Marsh, „Human-Computer-Human Interaction: Trust in CSCW," *SIGCHI Bulletin*, no. 29(3), pp. 36-40, 1997.

[256] E. L. Loftus, „Creating false memories", *Scientific American*, pp. 70-75, September 1997.

[257] E. Knapp, „Know-how's Not Easy: How to Keep knowledge management from flickering out," *ComputerWorld*, January 1997.

[258] L. J. Bannon and K. Kuutti, *Shifting perspectives on organizational memory: from storage to active remembering.*, 1996.

[259] H. Sorensen, A. O'Riordan, and C. O'Riordan, „Profiling with the INFOrmer Text Filtering Agent," *Journal of Universal Computer Science*, no. 3(8), pp. 988-1006, 1997.

[260] N. Khilwani and J. A. Harding, *Managing corporate memory on the semantic web*. New York: Springer Science+Business Media, 2014.

[261] K. Eason and W. Olphert, „Early evaluation of the organisational implications of CSCW systems", in *CSCW Requirements and Evaluation*. London: Springer, 1996, pp. 75-89.

[262] A. Macaulay, „Cooperation, requirements analysis and CSCW," in *CSCW Requirements and Evaluation*. London: Springer, 1996, pp. 39-55.

[263] A. Macintosh, „Knowledge Asset Management", *AIring*, April 1997.

[264] L. Karsenty. (1996) An empirical evaluation of design rationale documents, Electronic Proceedings of CHI'96. Document. [Online]. http://www.acm.org/sigchi/chi96/proceedings/papers/Karsenty/lk_txt.htm

[265] G. L. Urban and E. Von Hippel, „Lead user analyses for the development of new industrial products", *Management Science,* no. 34(5), pp. 569-582, 1988.

[266] M. S. Fox, „Issues in Enterprise Modelling. In Systems Engineering in the Service of Humans, Proceedings of the IEEE Conference on Systems, Man and Cybernetics", *IEEE Computer Society*, pp. 86-92, October 1993.

[267] M. Uschold, M. King , S. Moralee, and Y. Zorgios, „The Enterprise Ontology", *The Knowledge Engineering Review, Special Issue on Putting Ontologies to Use* , vol. XIII, 1998.

[268] J. Fraser, „Managing Change through Enterprise Models, Proceedings of Expert Systems'94," in *4th Annual Conference of the British Computer Society Specialist Group on Expert Systems*, Cambridge, 1994.

[269] D. Beauchène, S. Mahé, and C. Rieu, „Enterprise Know-How: Capitalization and Benchmarking with an Enterprise Organizational Model," in *Knowledge Management: Organization, Competence and Methodology, Proceedings of ISMICK'96*. Rotterdam, Wurzburg:Ergon, Netherlands, 1996, pp. 194-206.

[270] F. Maurer and B. Dellen, „A Concept for an Internet-based Process-oriented Knowledge Management Environment," in *Proceedings of the 11th Workshop on Knowledge Acquisition, Modeling and Management (KAW'98)*., 1998.

[271] N. Feray et al., *MnemosNet: a corporate memory system for the research laboratories, Proceedings of IC'98*. Pont-à-Mousson, France, 1998.

[272] T. Bollon, „Capitalisation des connaissances et conception: éléments de méthodologie," in *Connaissances et savoir-faire en entreprise: information et capitalisation*. Paris: Hermè, 1997, pp. 130-153.

[273] A. Wisner, *Anthropotechnologie: vers un monde industriel pluri-centrique*. Toulouse: Octarès, 1997.

[274] R. Banares-Alcantara and J. M. P. King, „Design support systems for process engineering. III. Design rationale as a requirement for effective design support.," *Computers and Chemical Engineering*, no. 21(3), pp. 263–276, 1997.

[275] C. Bourne, „Catégorisation et formalisation des connaissances industrielles," in *Connaissances et Savoir-faire en entreprise*.: Hermès, 1997, pp. 179-197.

[276] J. C. Corbel, „Méthodologie de retour d'experience: démarche MEREX de Renault", in *Connaissances et Savoir-faire en entreprise*.: Hermès, 1997, pp. 93-110.

[277] J. P. Poitou, „Documentation is Knowledge: An Anthropological Approach to Corporate Knowledge Management," in *SMICK'95*, Compiègne, 1995, pp. 91-103.

[278] J. F. Ballay and J. P. Poitou, „Diadème: a Collective Knowledge Management System", in *Knowledge Management: Organization, Competence and Methodology, Proc. of the 4th Int. Symposium on the Management of Industrial and Corporate Knowledge (ISMICK'96)*. Rotterdam, Netherlands: Wurzburg: Ergon Verlag, 1996, pp. 265-285.

[279] J. F. Ballay, *Capitaliser et transmettre les savoir-faire de l'entreprise*.: Eyrolles, 1997.

[280] D. E. O'Leary, „Knowledge management across the eterprise resource planning systems life cycle", *International Journal of Accounting Information Systems*, no. 3, pp. 99-10, 2002.

[281] D. E. O'Leary, „Using AI in Knowledge Management: Knowledge Bases and Ontologies", *IEEE Intelligent Systems*, no. 13(3), pp. 34-39, May-June 1998.

[282] E. C. Nevis, A. J. DiBella, and J. M. Gould, „Understanding Organizations as Learning Systems", *Sloan Management Review*, Winter 1995.

[283] L. Steels, „The componential framework and its role in reusability", in *Second Generation Expert Systems*. Berlin, Germany: Springer-Verlag, 1993, pp. 273-298.

[284] K. C. Kingston, „Modelling Business Processes using the Soft Systems Approach", in *Proceedings of the 2nd Int. Symposium on the Management of Industrial and Corporate Knowledge (ISMICK '94)*. Compiègne, 1994, pp. 149-159.

[285] R. Van der Spek, „Towards a methodology for knowledge management," in *Proceedings of the 2nd Int. Symposium on the Management of Industrial and Corporate Knowledge (ISMICK '94)*. Compiègne, 1994, pp. 93-102.

[286] O. Corby and R. Dieng, „Cokace: a Centaur-based environment for Common KADS Conceptual Modelling Language", in *Proceedings of the 12th European Conference on Artificial Intelligence (ECAI'96)*. Budapest, Hungary: John Wiley & Sons, 1996, pp. 418-422.

[287] R. Dieng, A. Corby, and M. Ribiere, *Methods and Tools for Corporate Knowledge Management*.: Institut National de Recherche en Informatique et en Automatique, INRIA, 1998.

[288] A. Abecker, A. Bernardi, K. Hinkelmann, O. Kühn, and M. Sintek, „Towards a Technology for Organizational Memories", *IEEE Intelligent System*, no. 13(3), pp. 40-48, May-June 1998.

[289] A. Farquhar, R. Fikes, and J. Rice, „The Ontolingua Server: a Tool for Collaborative Ontology Construction", in *Proceedings of KAW'96*. Banff, Canada, 1996, pp. 44-1 – 44-19.

[290] J. Tennison and N. R. Shadbolt, „APECKS: a Tool to Support Living Ontologies", in *Proceedings of the 11th Workshop on Knowledge Acquisition, Modeling and Management (KAW'98)*, 1998.

[291] G. Simon and M. Grandbastien, *Corporate knowledge: a case study in the detection of metallurgical flaws. Proceedings of ISMICK'9*. Compiègne, France, 1995.

[292] L. Admane, *A Generic Model of Corporate Memory: Application to the Industrial Systems*.: Institut National d'Informatique, Algeria, 1997.

[293] Ch. Djellali, *A new digital conceptual model oriented corporate memory constructing: Taking Data Mining models as a cas*.: The 3rd International Symposium on Frontiers in Ambient and Mobile Systems, 2013.

[294] B. R. Gaines, D. H. Norrie, A. Z. Lapsley, and M. L. G. Shaw, „Knowledge Management for Distributed Enterprises", in *Proceedings of KAW '96*., 1996, pp. 37-1 37-18.

[295] M. Ribière and N. Matta, „Virtual Enterprise and Corporate Memory", in *Proceedings of ECAI'98 Workshop on Building, Maintaning and Using Organizational Memories*., 1998, pp. 129-147.

[296] L. Vandenberghe and H. De Azevedo, *Multi-Agent Systems & Knowlege Capitalisation: an Overview, Proceedings of ISMICK'95*. Compiègne, France, 1995.

[297] J. Domingue, „Tadzebao and WebOnto: Discussing, Browsing, and Editing Ontologies on the Web", in *Proceedings of the 11th Workshop on Knowledge Acquisition, Modeling and Management (KAW'98)*., 1998, pp. 18-23.

[298] P. Martin and Alpay, L., „Conceptual Structures and Structured Document," in *Conceptual Structures: Knowledge Representation as Interlingua, ICCS'96*.: Springer-Verlag, 1996, pp. 145-159.

[299] P. Trigano, *Automatic Indexation and Knowledge Storing. Proceedings of ISMICK' 94*. Compiègne, France, 1994.

[300] R. Dieng, O Corby, A. Giboin, and M. Ribiere, „Methods and Tools for Corporate Knowledge Management," *Int. J. Human-Computer Studies*, no. 51, pp. 567-598, 1999.

[301] G. Bologna and J. Gameiro Pais, „ICARE: an operational knowledge management system.," in *5th Int. Symposium on the Management of Industrial and Corporate Knowledge (ISMICK'97)*, Compiègne, 1997, pp. 150-162.

[302] C. Revelli, *Intelligence stratégique sur Internet*.: Dunod, 1998.

[303] J. L. Ermine, *Les systemes de connaissances*. Paris: Hermes, 1996.

[304] T. McGuire, J. Manyika, and M. Chui, „Why Big Data is The New Competitive Advantage," *Ivey Business Journal*, no. 76(4), pp. 1-4, 2012.

[305] R. Heisterberg and A. Verma, *Creating Business Agility: How Convergence of Cloud, Social, Mobile, Video, and Big Data Enables Competitive Advantage*. San Francisco: John Wiley & Sons, 2014.

[306] M. Cox and D. Ellsworth, „Application-Controlled Demand Paging for Out-of-Core Visualization, Report NAS-97-010," NASA Ames Research Center, 1997.

[307] S. Weiss and N. Indurkhya, *Predictive Data Mining: A Practical Guide*.: Morgan Kaufmann Publishers Inc., 1998.

[308] M. Van Rijmenam, *Think Bigger, Developing a Successful Big Data Strategy for Your Business*.: AMACOM, 2014.

[309] D. Laney, *3D Data Management: Controlling Data Volume, Velocity and Variety, Application Delivery Strategies*.: META Group, 2001.

[310] J. Manyika et al., *Big Data: The next frontier for innovation, competition, and productivity*.: McKinsey Global Institute, 2011.

[311] J. Berman, *Principles of Big Data, Preparing, Sharing and Analyzing Complex Information*. Boston: Elsevier, 2013.

[312] T. Havens, J. Bezdek, C. Leckie, L. Hall, and M. Palaniswami, „Fuzzy c-Means Algorithms for Very Large Data," *IEEE Transactions on Fuzzy Systems*, no. 20(6), pp. 1130-1146, 2012.

[313] M. Rouse. (2016, january) Big data. Document. [Online]. http://www.sas.com/en_us/insights/big-data/what-is-big-data.html

[314] R. Buyya, N. R. Calheiros, and V. A. Dastjerdi, *Big Data Principles and Paradigms*.: Elsevier Inc., 2016.

[315] C. P. Chen and C. Y. Zhang, „Data-intensive applications, challenges, techniques and technologies: A survey on Big Data", *Information Sciences*, no. 275, pp. 314-347, 2014.

[316] Y. Zheng, F. Liu, and H. P. Hsieh, „U-Air: When urban air quality inference meets big data", in *9th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2013, pp. 1436-1444.

[317] V. Mayer-Schönberger and K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Canada: Eamon Dolan/Houghton Mifflin Harcourt, 2013.

[318] P. Lyman, H. R. Varian, J. Dunn, A. Strygin, and K. Swearingen, *How much information?*: UC Berkeley, 2003.

[319] R. Walker, *From Big Data to Big Profits, Success with Data and Analytics*. New York: Oxford University Press, 2015.

[320] H. Mintzberg. (2015, January) Managing in Digitale Age: Over the Edge? Document. [Online]. http://www.druckerforum.org/blog/?p=928

[321] M. Van Rijmenam, *Think Bigger, Developing a Successful Big Data Strategy for Your Business*.: AMACOM, 2014.

[322] M. Minelli, M. Chambers, and A. Dhiraj, *Big Data, Big Analytics*. New Jersey: John Wiley & Sons, 2013.

[323] A. McAfee and E. Brynjolfsson, „Big Data: The Management Revolution", *Harvard Business Review*, pp. 61-68, 2012.

[324] S. Kudyba and M. Kwatinetz, „Introduction to the Big Data Era", in *Big Data, Mining, and Analytics*.: CRC Press, Taylor & Francis Group, 2014, pp. 1-17.

[325] F. Zeller, C. Ponte, and B. O'Neill, *Revitalising in European Audience Research*. Routledge, New York, London: Taylor and Francis Group, 2014.

[326] B. Bilbao-Osorio, R. Crotti, S. Dutta, and B. Lanvin, „The Networked Readiness Index 2014: Benchmarking ICT Uptake in a World of Big Data", in *The Global Information Technology Report 2014, Rewards and Risks of Big Data*. Geneva: World Economic Forum, 2014, pp. 3-35.

[327] M. Schroeck, R. Shockley, J. Smart, D. Romero-Morales, and P. Tufano, *Analytics: The real-world use of big data. How innovative enterprises extract value from uncertain data*.: IBM Institute for Business Value, 2012.

[328] T. Davenport, *Big Data at Work: Dispelling the Myths, Uncovering the Opportunities*. Boston: Harvard Business Review Press, 2014.

[329] B. Marr, *Big Data: Using Smart Big Data, Analytics and Metrics to make Better Decisions and Improve Performance*. San Francisco: John Wiley & Sons, 2015.

[330] H. Sun and P. Heller, *Oracle Information Architecture: An Architect's Guide to Big Data*.: Oracle, 2012.

[331] D. Ho, B. Obel, and C. Snow, *Unleashing the potential of Big Data, A white paper based on the 2013 World Summit on Big Data and Organization Design*. Paris: IBM, Paris-Sorbonne University, ICOA, ODC, 2013.

[332] J. Gantz and D. Reinsel, *The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east*.: IDC iView: IDC Analyze the Futur, 2013.

[333] B. El-Darwiche, V. Koch, D. Meer, R. Shehadi, and W. Tohme , „Big Data Maturity: An Action Plan for Policymakers and Executives," in *The Global Information Technology Report 2014, Rewards and Risks of Big Data*. Geneva: World Economic Forum, 2014, pp. 43-53.

[334] T. Davenport and J. Harris, *Competing on Analytics, The New Science on Winning*. Boston: Harvard Business School Press, 2007.

[335] L. Taylor, R. Schroeder, and E. Meyer, „Emerging Practices and Perspectives on Big Data Analytics in Economics: Bigger and better or more of the same?," *Big Data & Society*, pp. 1-10, 2014.

[336] T. Erl, W. Khattak, and P. Buhler, *Big Data Fundamentals, Concepts, Drivers & Techniques*. Boston: Prentice Hall, 2016.

[337] A. Wright, „Mining the web for feelings, not facts," *The New-York Times*, August 23 2009.

[338] B. Beasens, *Analytics in a Big Data World, The Essential Guide to Data Science and its Applications*. New Jersey: John Wiley & Sons, 2014.

[339] M. Chen, S. Mao, Y. Zhang, and V. Leung, *Big Data Related Technologies, Challenges and Future Prospects*. London: Springer, 2014.

[340] P. Joshi, „Analyzing Big Data Tools and Deployment Platforms," *International Journal of Multidisciplinary Approach and Studies*, no. 2(2), pp. 45-56, 2015.

[341] N. Khan, I. Yaqoob, I. Hashem, and Z. Inayat, „Big Data: Survey, Technologies, Opportunities, and Challenges," *The Scientific World Journal*, 2014.

[342] E. Olshannikova, A. Ometov, Y. Koucheryavy, and T. Olsson, „Visualizing Big Data with augmented and virtual reality: challenges and research agenda," *Journal of Big Data*, no. 2(1), pp. 1-27, 2015.

[343] S. Wamba, S. Akter, A. Edwards, G. Chopin, and D. Gnanzou, „How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study," *International Journal of Production Economics*, no. 165, pp. 234-246, 2015.

[344] V. Charles and T. Gherman, „Achieving Competitive Advantage Through Big Data. Strategic Implications," *Middle-East Journal of Scientific Research*, no. 16(8), pp. 1069-1074, 2013.

[345] M. Vidas Bubanja, „Zašto je Srbiji potrebna digitalno podržana razvojna strategija," *Ekonomski vidici, tematski broj „Ka novoj privredi Srbije"*, no. 20(2/3), pp. 153-166, 2015.

[346] M. Berner, E. Graupner, and A. Maedche, „The Information Panopticon in The Big Data Era," *Journal of Organization Design,* no. 3(1), pp. 14-19, 2014.

[347] S. Poole, „The digital panopticon," *New Statesman*, no. 142(5159), pp. 23-25, 2013.

[348] A. Donovan, R. Finn, K. Wadhwa, L. Bigagli, and J.M. Garcia, *Big data road map and crossdisciplinary community for addressingsocietal externalities*.: European Union, 2014.

[349] C. McNeely and J. Hahm, „The Big (Data) Bang: Policy, Prospects, and Challenges," *Review of Policy Research*, pp. 304-310, 2014.

[350] R. Kitchin, *The Data Revolution: Big Data, open Data, Data Infrastructures & Their consequences*. London: SAGE Publications Ltd., 2014.

[351] S. Lund, J. Manyika, S. Nyquist, L. Mendonca, and S. Ramaswamy, *Game changers: Five opportunities for US growth and renewal*.: McKinsey Global Institute, McKinsey & Company, 2013.

[352] E. Siegel, *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die*. New Jersey: John Wiley & Sons, 2013.

[353] J. Goss, „We know who you are and we know where you live: the instrumental rationality of geodemographics systems," *Economic Geography*, pp. 171-185, 1995.

[354] J. Kobielus, „Humans vs. algorithms: Who - or what should decide?," *Info World*, p. 1, June 2015.

[355] M. Bolling and F. Zettelmeyer, *Big Data Doesn't Make Decisions: Leaders Do*.: Egon Zehnder International Inc., 2014.

[356] B. Marr, *Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results*.: John Wiley & Sons Inc., 2016.

[357] D. Helbing, *Thinking Ahead – Essays on Big Data, Digital Revolution and Participatory Market Society*. New York: Springer, 2015.

[358] C. Mader and R. Hagin, *Information systems: technology, economics, applications*. Chicago: Science Research Associates, 1974.

[359] C. Van Doren, *A History of Knowledge: The Pivotal Events and Achievement of World History*. New York: Ballantine Books, 1991.

[360] M. Castells, *The Rise of Network Society: The Information Age: Economy, Society and Culture, Vol. 1*. Oxford: Blackwell Publishers, 1996.

[361] R. Hillard, *Information Driven Business: How to Manage Data and Information for Maximum Advantage*. New Jersey: John Wiley & Sons, 2010.

[362] W. Dutton, „Continuity or Transformation? Social and Technical Perspectives on Information and Communication Technologies.," in *Transforming Enterprise, The Economic and Social Implications of Information Technology*. Cambridge: The MIT Press, 2005, pp. 13-24.

[363] C. Williams, *Principi menadžmenta – MGMT*. Beograd: Data status, 2010.

[364] K. Anderson, *Creating a Data-Driven Organization, Practical Advice from the Trenches*. Boston: O'Reilly, 2015.

[365] P. Géczy, „Big Data Management: Relational Framework," *Review of Business & Finance Studies*, no. 6(3), pp. 21-30, 2015.

[366] W. Pedrycz and S. Chen, *Information Granularity, Big Data, and Computational Intelligence*. Switzerland: Springer, 2015.

[367] R. Pepper and J. Garrity, „The Internet of Everything: How the Network Unleashes the Benefits of Big Data," in *The Global Information Technology Report 2014, Rewards and Risks of Big Data*. Geneva: World Economic Forum, 2014, pp. 35-43.

[368] C. Beath, I. Becerra-Fernandez, J. Ross, and J. Short, „Finding Value in the Information Explosion," *MIT Sloan Management Review*, no. 53(4), pp. 18-20, 2012.

[369] F. Provost and T. Fawcett, „Data Science and its Relationship to Big Data and Data-Driven Decision Making," *Big Data online journal*, no. 1(1), pp. 51-59, 2013.

[370] R. Adduci, D. Blue, G. Chiarello, J. Chickering, and D. Mavroyinnanis, *Big Data: Big Opportunities to Create Business Value*. Massachusetts: EMC Corporation, 2011.

[371] R. Kalakota and M. Robinson, *E-Business 2.0: Roadmap for Success*. New York: Addison – Wesley, 2001.

[372] M Rakić Skoković and D. Stefanović, „Unapređenje performantnosti organizacije, procesa i poslova uvođenjem ERP sistema," *Strategijski menadžment*, no. 1-2, pp. 182-186, 2005.

[373] M. G. Shields, *E-business and erp rapid implementation and project planning*.: John Wiley & Sons, Inc., 2001.

[374] N. Majdandžić, *Računalom integrirana proizvodnja*. Slavonski Brod: Sveučilište Josip Juraj Strossmayes, Strojarski fakultet, 1997.

[375] M. Al-Mashari, A. Al-Mudimigh, and M. Zairi, „Enterprise Resource Planning: A taxonomy of critical factors," *European Journal of Operational Research*, no. 2, pp. 352-364, 2003.

[376] K. Boersma and S. Kingma, „Developing a cultural perspective on ERP.," *Business Process Management Journal*, no. 11(2), pp. 123-136, 2005.

[377] H. Klaus, M. Rosemann, and G.G. Gable, „What is ERP?," *Information System Frontiers*, no. 2(2), pp. 141-162, 2000.

[378] Gartner Group, *New and Upcoming Research. Retrieved February*. Masterfile, 2000.

[379] K. Kwahk and H. Ahn, „Moderating effects of localization differences on ERP use: A socio-technical system perspective," *Computers in Human Behavior*, no. 2, pp. 186-198, 2010.

[380] E. Monk and B. Wagner, *Concepts in Enterprise Resource Planning, Third Edition*. Boston: Course Technology Cengage Learning, 2009.

[381] A. Leon, *ERP Demystified*. New Delhi: Tata McGraw Hill Publishing Co., 2008.

[382] APICS, *APICS Dictionary, 13th Edition*.: APICS, 2012.

[383] L. E. Colmenares and J. O. Otineo, *Critical Success Factors of ERP Implementation*.: Idea Group Inc., 2005.

[384] Z. A. Hasibuan and G. R. Dantes, „Priority of Key Success Factors (KSFS) on Enterprise Resource Planning (ERP) System Implementation Life Cycle," *Journal of Enterprise Resource Planning Studies*, p. 15, 2012.

[385] F. Nah and J. Lau, „Critical Factors for successful implementation of enterprise systems," *Business Process Management Journal*, vol. VII, no. 3, pp. 285-296, 2001.

[386] K. Al-Fawaz, Z. Al-Salti, and T. Eldabi, *Critical Success Factors in ERP Implementation: A Review*. Dubai: European and Mediterranean Conference on Information Systems, 2008.

[387] C. Doom and K. Milis , *CSFS of ERP implementations in Belgian SMEs: a multiple case study*. Izmir: European and Mediterranean Conference on Information Systems, 2009.

[388] T. H. Davenport, „Putting the Enterprise into the Enterprise System," *Harvard Business Review*, pp. 121-131, July-August 1998.

[389] F-H. N. Fiona, *Enterprise Resource Planning Solutions&management, IRM Press*. Hershey, USA: Rai Technology University, Enterprise Resource Planning, 2009.

[390] K. Kumar and J. V. Hillegersberg, „ERP Experience and Evolution," *Communications of the ACM*, no. 4, pp. 23-26, April 2000.

[391] H. M. Beheshti, „What managers should know about ERP/ERP II," *Management Research News*, no. 29, pp. 184-193, 2006.

[392] K. P. Tripathi, „Measuring the Performance of an ERP System," *International Journal of Computer Science and Technology*, vol. II, no. 3, September 2011.

[393] C. Sheu, H. R. Yen , and D. W. Krumwiede, „The effect of national differences on multinational ERP implementation: an exploratory study," *TQM & Business Excellence*, vol. XIV, no. 6, pp. 641-657, August 2003.

[394] P. Garg, „Critical Success factors for Enterprise Resource Planning implementation in Indian Retail Industry: An Exploratory study," *International Journal of Computer Science and Information Security*, vol. VIII, no. 2, 2010.

[395] J. W. Ross, P. Weil, and D. Robertson, *Enterprise Architecture as Strategy*. Boston: Harvard Business School Press, 2006.

[396] S. Dhiraj, *Foundation of Information Technology*. New Delhi: EXCEL BOOKS, 2008.

[397] B. Bond et al., *ERP is Dead – Long Live ERP II, Research Note*.: Gartner Group, 2000.

[398] T. F. Wallace and M. H. Kremzar, *ERP – Making it Happen*. New York: John Wiley & Sons Inc., 2001.

[399] S. H. Chung and C. A. Snyder, „ERP adoption: a technological evolution approach," *International Journal of Agile Management Systems*, no. 2/1, pp. 24-32, 2000.

[400] K. Parker, „The enterprise endeavor," *Manufacturing Systems*, vol. XIV, no. 1, pp. 14-20, January 1996.

[401] T. F. Wallce, *MRP II: Making it Happen*.: Oliver Wight Limited Publications, Essex Juniction, 1985.

[402] H. R. HassabElnaby, W. Hwang, and M. A. Vonderembse, „The impact of ERP implementation on organizational capabilities and firm performance, Benchmarking," *An International Journal*, vol. XIX, no. 4/5, pp. 618-633, 2012.

[403] J. Darlington and C. Moar, „MRP rest in peace," *Management Accouting*, no. 9, pp. 74-92, 1996.

[404] Y. Yusuf and D. Little, „An empirical investigation of enterprise-wide integration of MRP II," *International Journal of Operations & Production Management*, vol. XVIII, no. 1, pp. 66-86, 1998.

[405] I. J. Chen, „Planning for ERP systems: analysis and future trend," *Business Process Management Journal*, vol. VII, no. 5, pp. 374-386, 2001.

[406] C. Koch, *ERP-systemer, erfainger, resourcer, forandringer. (in Danish: ERP Systems – expiriences, resources, change)*. Copenhagen: Ingenioren-boger, 2007.

[407] B. Neverauskas and V. Stankevicius, *Project management: research and studies at the faculty of economics and management*. Kaunas: Kaunas University of Technology // Engineering economics , 2008.

[408] J. O. Chan, *E-business enabled ERP II architecture*.: Communications of the International Information Management Association, 2010.

[409] M. Bradford, *Modern ERP, Select, Implement & use today`s advanced business systems*. Raleigh: NC, Copyright, 2015.

[410] V. Kumar, B. Maheshwari, and U. Kumar, „ERP systems implementation: Best practices in Canadian government organizations," *Government Information Quarterly*, no. 19, pp. 147–172, 2002.

[411] E. A. Khvalev. (2010, January) Key Risks in ERP Implementation, Identification and Analysis by Project Phases. Document. [Online]. http://imtcj.ac.in/ITBI%2010%20Proceedings/Book/28.pdf

[412] M. Haddara, *ERP Adoption Cost Factors in SMEs, European*. Athens, Greece: Mediterranean Eastern Conference on Information Systems 2011, 2011.

[413] A. Boonostra, „Interpreting an ERPimplementation project from a stakeholder perspective," *International Journal of Project Management,* vol. XXIV, pp. 38-52, 2006.

[414] Y. Yusuf, A. Gunasekaran, and C. Wu, „Implementation of enterprise resource planning in China," *Technovation*, no. 26, pp. 1324-1336, 2006.

[415] H. R. HassabElnaby, W. Hwang, and M. A. Vonderembse, „The impact of ERP implementation on organizational capabilities and firm performance," *Benchmarking: An International Journal*, vol. XIX, no. 4/5, pp. 618-633, 2012.

[416] A. Parr and G. Shanks, „A Model of ERP Project Implementation," *Journal of Information Technology*, vol. XV, no. 2, pp. 289-303, 2000.

[417] N. Nawaz and K. Channakeshavalu, „The Impact of Enterprise Resource Planning (ERP) Systems Implementation on Business Performance," *Asia Pacific Journal of Research*, vol. II, no. 4, 2013.

[418] [Online].www.vidilab.com magazin

[419] Službena stranica SAP proizvođača.. [Online]. http://go.sap.com/croatia/index.html

[420] M. Hobo and C. Watanabe, *Creating a Firm Self-propagating Function for Advanced Innovation-oriented projects:lessons form ERP*.: Technovation, 2004.

[421] Z. Yajun, *Risk Management for Enterprise Resource Planning System Implementations in Project Based Firms*. USA, 2010.

[422] „Implementing SAP Solutions on Amazon Web Services Created by: Amazon Web Services LLC sap-onaws@amazon.com Version: 3 – April 2013,".

[423] S-W. Chou and Y-C. Chang, „The implementation factors that influence the ERP (enterprise resource planning) benefits," *Decision Support Systems*, no. 46, pp. 149-157, 2008.

[424] D. Vasiljević and B. Jovanović, *Menadžment logistike i lanaca snabdevanja*. Beograd: Fakultet organizacionih nauka, 2008.

[425] R. Kimball and M. Ross, *The Data Warehouse Toolkit, Third Edition, The Definitive Guide to Dimensional Modeling*. Canada: John Wiley & Son, Inc., 1996.

[426] V. Rainardi, *Building a Data Warehouse with Examples in SQL Server*.: Apress, 2008.

[427] W.H. Inmon, *Building the Data Warehouse, Third Edition*.: John Wiley & Son, Inc., 2002.

[428] Stanford. (2003, January) Stanford Web site. [Online]. https://web.stanford.edu/dept/itss/docs/oracle/10g/server.101/b10736/concept.htm#i1006297

[429] M. Breslin, „Data Warehousing Battle of the Giants: Comparing the Basics of the Kimball and Inmon Models," *Business Intelligence Journal*, Winter 2004.

[430] G. M. Marakas, *Modern Data Warehousing, Mining, And Visualization*.: Prentice Hall, 2003.

[431] R. Kimball and J. Caserta, *The Data Warehouse ETL Toolkit: Practical Techniques for Extracting, Cleaning, Conforming and Delivering Data*. Indianapolis: Wiley Publishing, 2004.

[432] C. Vercellis, *Data Warehousing, in Business Intelligence: Data Mining and Optimization for Decision Making*.: John Wiley & Sons, Ltd, 2009.

[433] B. Becker, (2009) Six Key Decisions for ETL Achitectures. [Online]. http://www.ralphkimball.com/html/articles.html

[434] Data Warehousing Gotchas. [Online]. http://www.dwininfocenter.org/gotchas.html

[435] C. Howson, *Successful business intelligence*. New York: McGraw Hill, 2008.

[436] S. Nagabhushana, *Data Warehousing: OLAP and Dana Mining*. New Delhi: New Age International, 2006.

[437] P. Kočović, *Računarstvo u oblaku, Internet ogledalo – Business & Technologies magazine – IT za direktore, spec. izdanje*.: GM Business & Lifestyle, 2005.

[438] Department of Commerce, USA) NIST (National Institute of Standards and Technology, *Special Publication 800-145*.: NIST, 2011.

[439] L. Badger, T. Grance , R. Patt-Corner, and J. Voas , *Cloud Computing Synopsis and Recommendations*. USA: National Institute of Standards and Technology, 2012.

[440] C. D. Plummer, J. T. Bittman, T. Austin, W. D. Cearley, and D. M. Smith, *Cloud Computing: Defining and Describing an Emerging Phenomenon*.: Gartner, 2008.

[441] M. Veinović and A. Jevremović, *Uvod u računarske mreže*. Beograd: Univerzitet Singidunum, 2008.

[442] E. F. Gillett, G. E. Brown , J. Staten, and Ch. Lee, *Future View: The New Tech Ecosystems Of Cloud, Cloud Services, and Cloud Computing: Understanding, Segmenting, and Competing in the Next Computer Revolution*.: Forrester Research, 2008.

[443] A. Bhadani and D. Jothimani, „Big Data: Challenges opportunities and realities," in *Effective Big Data Management and Opportunities for Implementation*. Pennsylvania, USA: IGI Global, 2016, pp. 1-24.

[444] D. Zeng, L. Gu, and S. Guo, *Cloud Networking for Big Data*. Switzerland: Springer International Publishing , 2015.

[445] R. Buyya, C. S. Yeo, S. Venugopal, J. Brobarg, and I. Brnadic, „Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, no. 25, pp. 599-616, 2009.

[446] A. S. Tanenbaum and M. Van Steen, *Distributed Systems: Principles and Paradigms, Second Edition*.: Prentice Hall, 2007.

[447] NIST. (2011) NIST Cloud Computing Reference Architecture. [Online]. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

[448] F. Liu et al., *NIST Cloud Computing Reference Architecture, Special Publication 500-292*. Gaithersburg, USA: NIST National Institute of Standards and Technology, 2011.

[449] K. K. R. Choo, *Cloud computing: Challenges and future directions, Trends & issues in crime and criminal justice, No. 400*. Australia: Australian Institute of Criminology, 2010.

[450] K. Hausman, L. S. Cook, and T. Sampaio, *Cloud Essentials, CompTIA Autorized Courseware for Exam CLO-001*. Indianapolis, Indiana: John Willey & Sons, Inc., 2013.

[451] ITU-T Focus Group. (2014) ITU-T Focus Group on Cloud Computing. [Online]. http://www.itu.int/en/ITU-/focusgroups/cloud

[452] H. Jin et al., „Tools and technologies for building clouds," *Cloud Computing*, Springer-Verlag, 2010, pp. 3-20.

[453] I. M. Abbadi, *Cloud Management and Security*. UK: University of Oxford, John Wiley & Sons, Ltd., 2014.

[454] D. Sarna, *Implementing and Developing Cloud Computing Applications*. Boca Raton: FL: Auerbach, 2011.

[455] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy, First edition*. USA: O'Reilly, 2009.

[456] S. Carlin and K. Curran, „Cloud Computing Security," *International Journal of Ambient Computing and Intelligence*, pp. 14-19, January-March 2011.

[457] P. Mell and T. Grance, *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*. USA: NIST – National Institute of Standards and Technology, 2011.

[458] ENISA, *Benefits, risks and recommendations for information security, Cloud Computing*.: ENISA, Cloud Security and Resilience Expert Group, 2009.

[459] CA Technologies. (2012) Cloud Platform. [Online]. http://www.ca.com/us/cloud-platform.aspx

[460] R. Bakhshi and J. Deepak, „Cloud Computing – Transforming the IT Ecosystem," *SETLabs Briefings*, vol. VII, no. 7, pp. 3-10, 2009.

[461] ENISA, *Cloud Computing Risk Assessment*.: ENISA, Security and Resilience Expert Group, 2009.

[462] T. White, *Hadoop – The Definitive Guide*. USA: O'Reilly, 2012.

[463] D. Zburivsky, *Hadoop cluster deployment*. UK: Packt Publishing, 2013.

[464] K. G. Srinivasa and A. K. Muppalla, *Guide to high performance distributed computing: case studies with hadoop, scalding and spark*. Germany: Springer, 2015.

[465] SAS Institute Inc. (2014) Hadoop: What is it and why does it matter?. [Online]. http://www.sas.com/en_us/insights/big-data/hadoop.html.

[466] B. Steele, J. Chandler, and S. Reddy, *Algorithms for data science. 1st edition*. Cham: Springer, 2016.

[467] EMC-Education Services, *Data Science & Big Data Analytics: Discovering, Analyzing, Visualizing and Presenting Data. 1st edition*. Indianapolis: John Wiley & Sons, Inc., 2015.

[468] Z. Voulgaris, *Data Scientist: The Definitive Guide to Becoming a Data Scientist*.: Technics Publications, 2014.

[469] G. K. Lockwood. (2015) Conceptual Overview of Map-Reduce and Hadoop. [Online]. http://www.glennklockwood.com/data-intensive/hadoop/overview.html.

[470] A. S. Achari, *Hadoop Essentials*. Birmingham – Mumbai: PACKT Publishing, 2015.

[471] M. M. Mois, *Apache Hadoop Tutorial, The Ultimate Guide*.: Web Code Geeks, Exelixis Media P.C., 2016.

[472] P. Julio, *Big Data Analytics with Hadoop*.: LinkedIn Corporation, 2009.

[473] S. Ryza, U. Laserson, S. Owen, and J. Wills, *Advanced Analytics with Spark*. Sebastopol, CA: O'Reilly Media Inc., 2015.

[474] A. Serafini, *Apache Solr beginner's guide, configure your own search engine experience with real-world data with this practical guide to Apache Solr*. UK: Packt Publishing, 2013.

[475] R. D. Schneider, *Hadoop Buyer's Guide*.: Ubuntu, 2013.

[476] Security and protection system. (2015) [Online]. https://www.britannica.com/technology/security-and-protection-system

[477] B. Blakley, E. McDermott, and D. Geer. (2001) Information security is information risk management. Document. [Online]. http://ns2.datacontact.dc.hu/~mfelegyhazi/courses/EconSec/readings/03_Blakley2001infosec.pdf

[478] ISO/IEC 17799. [Online]. https://www.iso.org/standard/33441.html.

[479] ISO/IEC. (2013) ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls. Document. [Online]. http://www.iso27001security.com/html/27002.html

[480] NASA. (2013) Information Technology Threats and Vulnerabilities. Document. [Online]. http://www.hq.nasa.gov/security/it_threats_vulnerabilities.htm

[481] CIS. (2006) Osnove_upravljanja_rizikom. Document. [Online]. http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf.

[482] CERT, *Smernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika*. Zagreb: Nacionalni CERT, 2006.

[483] Y. Farah. (2013) Information technology 0150 Security techniques – Code of practice for information security controls. Document. [Online]. http://www.slideshare.net/YounessFarah/iso-iec-270022013-code-of-practice-for-is-management-original

[484] S. Stojaković. (2013) *Osnove upravljanja rizikom informacijskog sustava*. Document. [Online]. http://www.cis.hr/files/Celuska-Osnove_upravljanja_rizikom.pdf

[485] R. T. Stacey, Helsley, E. R., and V. J. Baston. (2006) Identifying Information Security Threats. Document. [Online]. http://www.ittoday.info/AIMS/DSM/82-10-41.pdf

[486] J. Aycock, *Computer Viruses and Malware*.: Springer, 2006.

[487] K. Thompson, „Reflections on trusting trust," *Communication ACM*, vol. XXVII, no. 8, pp. 761–763, August 1984.

[488] M. Jakobsson and R. Zulfikar, *Crimeware: Understanding New Attacks and Defenses*.: Addison Wesley Professional, 2008.

[489] M. Milosavljević, M. Veinović, and G. Grubor, *Informatika*. Beograd: Univerzitet Singidunum, 2009.

[490] M. Veinović and A. Jevremović, *Računarske mreže, peto izmenjeno i dopunjeno izdanje*. Beograd: Univerzitet Singidunum, 2016.

[491] N. Lord. (2012) Malware types. Document. [Online]. http://blog.veracode.com/2012/10/common-malware-typescybersecurity-101/

[492] P. J. Anderson, *Computer security technology planning study*. *Technical Report ESD-TR-73-51*.: Anderson (James P) & Co., 1972.

[493] F. Cohen, „Computer Viruses," University of Southern California, PhD Thesis 1986.

[494] V. J. Neumann, *Theory and organization of complicated automata*.: Burks, 1966.

[495] F. Cohen, *Computer Viruses: Theory and Experiments*.: Fred Cohen & Associates, 1984.

[496] M. Ananda, *Digital Security: Cyber Terror and Cyber Security*. New York: Infobase Publishing, 2010.

[497] M. Bishop, *Introduction to Computer Security*.: Addison-Wesley Professional, 2004.

[498] P. B. Pathak, „A Dangerous Trend of Cybercrime: Ransmoware Growing Challenge," *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, vol. V, no. 2, 2016.

[499] TrendLabs Trend Micro, *Ransomware Past, Present, and Future*.: Technical Marketing Team, 2017.

[500] Cisco-Talos. (2016, April) Ransmoware: Past, Present, and Future. Document. [Online]. http://blog.talosintel.com/2016/04/ransomware.html

[501] J. Wyke and A. Ajjan, *The Current State of Ransomware*.: SophosLabs technical paper, 2015.

[502] A. Allievi, H. Unterbrink, and W. Mercer, *CryptoWall 4.0 the Evolution Continues*.: Cisco Talos white paper, 2016.

[503] P. B. Pathak, „A Dangerous Trend of Cybercrime: Ransmoware Growing Challenge," *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, vol. V, no. 2, 2016.

[504] B. Lee, *Ransomware: Unlocking the Lucrative Criminal Business Model*.: Palo Alto Networks, Inc., 2016.

[505] Web Guard brošura. [Online]. http://www.towersnet.rs/wp-content/uploads/2015/06/Web-Guard-flyer.pdf.

[506] T. A. Roebuck. Computer Crime Research Center, Network security: DoS vs DDoS attacks. [Online]. http://www.crime-research.org/articles/network-security-dos-ddos-attacks

[507] NCERT, „NCERT-PUBDOC, Zero day ranjivosti," Nacionalni CERT, Zagreb, 2010.

[508] Attorney General of New Jersey. (2000) COMPUTER CRIME, A Joint Report, Commission of Investigation. [Online]. http://www.state.nj.us/sci

[509] T. Bidwell, *Hack Proofing Your Identity in the Information Age*. Rockland: Syngress Publishing, 2002.

[510] D. Pleskonjić, V. Milutinović, N. Maček, B. Đorđević, and M. Carić, „Psychological profile of network intruder," in *IPSI 2006*, Amalfi, Italy, 2006, pp. 23-26.

[511] R. Shirey, *Internet Security Glossary, Version 2*.: RFC , 2007.

[512] J. K. Jones, R. Bejtlich, and W.C. Rose, *Real Digital Forensics: Computer Security and Incident Response*.: Addison-Wesley Professional, 2005.

[513] R. J. Vacca, *Computer and Information Security Handbook, 3rd Edition*. USA: Elsevier, , 2017.

[514] NCERT, *CERT sistematizacija i način povezivanja svih faktora u sekvenci ugrožavanja bezbednosti*. Zagreb: Nacionalni CERT, 2010.

[515] S. McClure, J. Scambray, and G. Kurtz, *Hakerske tajne: zaštita mrežnih sistema, prevod 5. izdanja*. Beograd: Mikro knjiga, 2005.

[516] R. S. Petrović, *Kompjuterski kriminal*, Beograd: Vojnoizdavački zavod, 2004.

[517] E. K. Anderson, *International Intrusions: Motives and Patterns, The Proceedings of the 1994 Bellcore/Vell South Security Symposium*., 1994.

[518] R. Blake, I. Davis, B. Sterling, and M. Tenhuen, „Combating Computer Crime," *Interpol Review, No 417 (Confidential Supplement)*, no. 11, p. 10, 1989.

[519] CLS, „Threats to Computer Systems: An Overview," *CLS – Computer Systems Laboratory Bulletin*, 1994.

[520] R. L. Krutz and R. D. Vines, *The Cissp Prep Guide: Mastering the Ten Domains of Computer Security*.: John Wiley & Sons, 2000.

[521] J. Harriman, *A Testing Methodology for Antispyware Products Removal Effectiveness, Whitepaper Symantec Security Response*. Dublin, Ireland: Symantec, 2006.

[522] H. C. Malin, E. Casey, and M.J. Aquilina, *Malware Forensics: Investigating and Analyzing Malicious Code*.: Syngress, 2008.

[523] P. C. Pfleeger and L.S. Pfleeger, *Security in Computing, 3rd edition*.: Prentice Hall Professional Techical Reference, 2003.

[524] M. Stamp, *Information security: principles and practice*. USA: John Wiley & Sons, 2006.

[525] E. Skoudis and T. Liston, *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, 2nd edition*.: Prentice Hall, 2006.

[526] Matos. da Silva Pires. de Moraes. Alexandre, *Cisco Firewalls*. USA: Cisco Systems, Inc., 2011.

[527] B. Schneier, *Secrets & Lies: Digital Security in a Networked World*.: John Wiley & Sons, 2000.

[528] D. E. Zwicky, S. Cooper, and D. B. Chapman, *Buidling Internet Firewalls, 2nd edition*.: O'Reilly Media, 2000.

[529] A. R. Deal, *Cisco Router Firewall Security*.: Cisco Press, 2004.

[530] D. E. Zwicky, S. Cooper, and D. B. Chapman, *Building Internet Firewalls, 2nd Edition*.: O'Reilly Media, 2001.

[531] S. Mrdović, *Sigurnost računarskih sistema*.: Elektrotehnički fakultet, Univerzitet u Sarajevu, 2014.

[532] U. Tupakula, V. Varadharajan, and N. Akku, „Intrusion detection techniques for infrastructure as a service cloud," in *IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC)*, Sydney, Australia, 2011, pp. 744–751.

[533] A. Alazab, M. Hobbs, J. Abawajy, A. Khraisat, and M. Alazab, „Information Management & Computer Security," *Library, Information Science & Technology Abstract*, vol. XXII, no. 5, pp. 431-449, 2014.

[534] K. Vieira, A. Schulter, and C. B. Westphall, „Westphall,C.M. Intrusion detection for grid and cloud computing," *IT Profesional*, vol. XII, pp. 38–43, 2010.

[535] S. Lodin, *Intrusion detection product evaluation criteria. Technical report*.: Ernst & Young LLP, 1998.

[536] R. Bace and P. Mell, *Intrusion Detection Systems. Technical Report NIST Special Publication 800-31*. USA: NIST, 2001.

[537] M. Bishop, *Introduction to Computer Security*.: Addison-Wesley Professional, 2004.

[538] P. J. Anderson, *Computer security threat monitoring and surveillance. Technical report*. Fort Washington, Pennsylvania: James P. Anderson Company, 1980.

[539] E. D. Denning, „An intrusion-detection model. Software Engineering," *IEEE Transactions*, vol. XIII, no. 2, pp. 222–232, 1987.

[540] D. Pleskonjić, N. Maček, B. Đorđević, and M. Carić, *Sigurnost računarskih sistema i mreža*, Beograd: Mikro knjiga, 2007.

[541] D. Wang and Z. Zhou, „Application of cloud model in intrusion detection," in *2nd International Conference on e-Business and Information SystemSecurity (EBISS)*, Wuhan, China, 2010, pp. 1-4.

[542] M. Barreno, B. Nelson, R. Sears, D. A. Joseph, and D. J. Tygar, „Can machine learning be secure?," in *ACM Symposium on Information, computer and communications security, ASIACCS'06*, New York, NY, USA, 2006, pp. 16–25.

[543] Top Layer Networks, *Beyond IDS: Essentials of Network Intrusion Prevention*.: Top Layer Networks, Inc., 2002.

[544] N. Maček, *Detekcija upada mašinskim učenjem / Machine Learning in Intrusion Detection*, Beograd: Zadužbina Andrejević, 2015.

[545] J. Brentano et al., „A system for distributed intrusion detection," *Compcon Spring '91. Digest of Papers*, pp. 170–176, 1991.

[546] L. T. Heberlein et al., „A network security monitor, Research in Security and Privacy," in *IEEE Computer Society Symposium on 1990* , 1990, pp. 296–304.

[547] C. Te-Shun, „Security threats on Cloud Computing vulnerabilities," *International Journal of Computer Science & Information Technology (IJCSIT)*, vol. V, no. 3, June 2013.

[548] A. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd edition*.: Wiley, 2008.

[549] P. Mell, V. Hu, R. Lippmann, J. Haines, and M. Zissman, *An Overview of Issues in Testing Intrusion Detection Systems. Technical Report NISTIR 7007*. USA: NIST, 2003.

[550] P. Lindstrom, *Intrusion Prevention Systems (IPS): next generation firewalls, Spire Research Raport*.: Spire, 2004.

[551] Secure Computing Corporation, *Intrusion Prevention Systems (IPS), Part one: Deciphering the inline Intrusion Prevention hype, and working toward a real-world, proactive security solution*.: Secure Computing Corporation, 2003.

[552] NIST and E. Aroms, *NIST Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)*. Paramount, CA: CreateSpace, 2012.

[553] A. S. Ashoor and S. Gore, „Difference between intrusion detection system (ids) and intrusion prevention system (ips),” in *Advances in Network Security and Applications, Proceedings of the 4th International Conference, CNSA 2011*.: Springer, 2011.

[554] NSS Group, *Intrusion Prevention Systems (IPS)*., 2004.

[555] N. Desai, *Intrusion Prevention Systems: the Next Step in the Evolution of IDS*., 2003.

[556] Host Intrusion Prevention Systems. (2005) [Online]. http://www.networkintrusion.co.uk/hips.htm

[557] Network Intrusion Prevention Systems. (2005) [Online]. http://www.networkintrusion.co.uk/inline.htm

[558] K. Scarfone and P. Mell, *Guide in Intrusion Detection and Prevention Systems, Special Publication 800-94*. USA: NIST, 2007.

[559] sans.org. [Online]. http://www.sans.org/politics.html

[560] R. Ross and S. Katzke , *NIST SP 800–53, A, B, C, Recommended Security Controls for Federal IS*.: NIST, 2005.

[561] G. Grubor and M. Milosavljević, *Osnovi bezbednosti informacija – Metodološko-tehnološke osnove*, Beograd: Univerzitet Singidunum, 2010.

[562] SANS Institute, *Information Security Policies & Best Practices*.: SANS Institute, 2009.

[563] ISF, *The Standard for Good Practice for Information Security*.: ISF, 2007.

[564] B. Guttman and E. Roback, *NIST SP 800–12 Rev. 1, An Introduction to Computer Security: The NIST Handbook*. USA: NIST, 2017.

[565] „Službeni glasnik RS” 6/2016. *Zakon o informacionoj bezbednosti*., 2016.

[566] D. Icove, K. Seger, and W. VonStroch, *Computer Crime A Crimefighter's Handbook*.: O'Reilly & Associates, 1995.

[567] E. Cole, R. Krutz, and J.W. Conley, *Network Security Bible*. Indianapolis: Wiley Publishing, 2005.

[568] W. Mao, *Modern Cryptography: Theory and Practice*. New Jersey: Prentice Hall PTR, 2004.

[569] N. Galbreath, *Cryptography for Internet and Database Applications*. Indianapolis: Wiley Publishing, 2002.

[570] H. Van Tilborg, *Encyclopedia of Cryptography and Security*. New York: University of technology Eindhoven, 2005.

[571] J. A. Menezes, A. S. Vanstone, and C. P. Van Oorschot, *Handbook of Applied Cryptography, 1st edition*. Boca Raton, USA: CRC Press, Inc., 1996.

[572] F. Piper and S. Murphy, *Cryptography: A very short Introduction*.: Oxford University Press, 2002.

[573] M. Veinović and S. Adamović, *Kriptologija I – Osnove za analizu i sintezu šifarskih sistema, prvo izdanje*. Beograd: Fakultet za informatiku i računarstvo, Univerzitet Singidunum, 2013.

[574] J.A. Buchmann, *Introduction to Cryptography*. New York: Technical University Dramstadt, 2002.

[575] M. Milosavljević and S. Adamović, *Kriptologija II – Osnove za analizu i sintezu šifarskih sistema, prvo izdanje*. Beograd: Univerzitet Singidunum, 2014.

[576] D. Khahn, *The Codebreakers: The story of Secret Writing*. New York: Macmillan Publishing Co., 1957.

[577] D. Kahn, *Kahn on Codes*. New York : Macmillan Publishing Co., 1983.

[578] Rh. M. Young, *Internet Security Cryptographic principles, algorithms and protocols*. Wiltshire: School of Electrical and Computer Engineering Seoul, John Wiley & Sons, 2003.

[579] S. Sinkovski and B. Lučić, *Informaciona bezbednost i kriptografija*.: Jugoimport SDPR Beograd, 2006.

[580] A. B. Forouzan and F. S. Chung, *TCP/IP Protocol Suite, 3rd edition*. New York: Mc Graw Hill book, 2006.

[581] Bureau of Standards. National, *Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46*. Washington: FIPS, 1977.

[582] B. Schneier, *Applied Cryptography, Protocols, Algorithms, and Source Code in C, 2nd edition*.: Wiley Publishing, Inc., 1996.

[583] Bureau of Standards. National, *DES Modes of Operation, NBS FIPS PUB 81*.: U.S. Department of Commerce, 1980.

[584] National Standards Institute. American, *American National Standard for Information Systems – Data Encryption Algorithm - Modes of Operation, ANSI X3.106*.: ANSI, 1983.

[585] M. Davio, Y. Desmedt, J. Goubert, F. Hoornaert, and J.-J. Quisquater, *Efficient Hardware and Software Implementation of the DES, Advances in Cryptology: Proceedings of CRYPTO 84*.: Springer- Verlag, 1984.

[586] F. Hoornaert, J. Goubert, and Y. Desmedt, *Efficient Hardware Implementation of the DES, Advances in Cryptology: Proceedings of CRYPTO 84*.: Springer-Verlag, 1984.

[587] M. Bishop, „An Application for a Fast Data Encryption Standard Implementation," *Computing Systems*, vol. I, no. 3, pp. 221-254, 1988.

[588] A. G. Broscius and J. M. Smith, *Exploiting Parallelism in Hardware Implementation of the DES, Advances in Cryptology – CRYPTO '91*.: Springer-Verlag, 1992.

[589] Institute of Standards and Technology. National, *Data Encryption Standard (DES), Federal Information Processing Standards Publication (FIPS PUB) 46-3*.: FIPS, 1999.

[590] W. Diffie and E. M. Hellman, „Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *Computer*, vol. X, no. 6, pp. 74-84, 1977.

[591] K. W. Campbell and M. J. Wiener, *DES Is Not a Group, Advances in Cryptology - CRYPTO '92*.: Springer- Verlag, 1993.

[592] E. Biham and A. Shamir, *Differential Cryptoanalysis of the Data Encryprion Standard*.: Springer, 1993.

[593] M. Matsui and A. Yamagishi, *A New Method for Known Plaintext Attack of FEAL Cipher*.: Springer, 1993.

[594] W. Diffie and M. E. Hellman, „New Directions in Cryptography," *IEEE Transactions on Information Theory*, pp. 644-654, November 1976.

[595] A. W. Shay, *Understanding data communications and networks*.: University of Wisconsin, 2004.

[596] M. Rosing, *Implementing elliptic curve cryptography*.: MANING, 1999.

[597] S. Adamović, *Zaštita informacionih sistema*, Beograd: Univerzitet Singidunum, 2015.

[598] A. Behrouz and S.Ch.F. Forouzan, *TCP/IP Protocol Suite, 3rd edition*.: Mc Graw Hill book, 2006.

[599] R. L. Rivest, A. Shamir , and L. M. Adleman, „A Method for Obtaining Digital Signatures and Publik-Key Cryptosystems«," *Communications of the ACM*, vol. XXI, no. 2, pp. 120-126, 1978.

[600] R.L. Rivest, A. Shamir, and L.M. Adleman, *On Digital Signatures and Publik-Key Cryptosystems. Technical Report, MIT/LCS/TR-212*.: MIT Laboratory for Computer Science, 1979.

[601] M. Gardner, „A New Kind of Cipher That Would take Millions of Years to Break," *Scientific American*, no. 8, pp. 120-124, 1977.

[602] M. J. Hinek, *Cryptoanalysis of RSA and its variants*. Boca Raton, London, New York: Chapman&Hall/CRC, Taylor&Francis Group, 2010.

[603] E. M. Helman, „The Matematics of Publik-Key Cryptography," *Scientific American*, no. 8, pp. 146-157, 1979.

[604] Y. Y. Song, *Cryptoanalytic Attacks on RSA*, UK and massachusetts Institute of Technology University of Bedfordshire, Ed. USA: Springer Science+Business Madia, LL., 2008.

[605] S. Katzenbeisser, *Recent Advances in RSA Cryptography*, Vienna University of Technology, Ed. Vienna, Austria: Springer Science+Business Media, LLC., 2001.

[606] D. Coppersmith, M. K. Franklin, J. Patarin, and M. K. Reiter, „Low-exponent RSA with related messages," in *Advances in Cryptology - EuroCrypt '96*. Berlin: Springer-Verlag, 1996, pp. 1-9.

[607] W. Stallings, *Cryptography and Network Security, 5th edition*. USA: Prentice Hall, 2011.

[608] C. K. Wu and X. M. Wang, „Determination of the True Value of the Euler Totient Function in the RSA Cryptosystem from a Set of Possibilities," *Elctronics Letters*, vol. XXIX, no. 1, pp. 84-85, 1993.

[609] A. Alexi, B.-Z. Chor, O. Goldreich, and C. P. Schnorr, „RSA and Rabin Functions Certain Parts are as hard as the Whole," *SIAM Journal on Computing*, vol. XVII, no. 2, pp. 194-209, 1988.

[610] A. Alexi, B.-Z. Chor, O. Goldreich, and C. P. Schnorr, „RSA and Rabin Functions Certain Parts are as hard as the Whole," *SIAM Journal on Computing*, vol. XVII, no. 2, pp. 194-209, 1988.

[611] W. H. Payne, *Publik Key Cryptography Is Easy to Break*., 1990.

[612] A. Shamir and E. Tromer, *Factoring Large Numbers with the TWIRL Device*., 2003.

[613] E. Barker, *NIST Special Publication 800-57: Recommendation for Key Management. Part 1: General Guideline, Revision 4*.: NIST - Computer Security, 2016.

[614] D. Freeman, „Time Without End: Physics and Biology in an Open Universe," *Reviews of Modern Physics*, no. 3, pp. 447-460, 1979.

[615] T. Kleinjung et al., *Factorization of a 768-bit RSA modulus*., 1996.

[616] M. J. Wiener, „Cryptanalysis of Short RSA Secret Exponents," *IEEE Transactions on Information Theory*, vol. XXXVI, no. 3, pp. 553–558, 1990.

[617] D. Boneh and G. Durfee, „Cryptanalysis of RSA with private key d less than N0,292," *IEEE Transactions on Information Theory*, vol. LXVI, no. 4, pp. 1339-1349, 2000.

[618] D. Boneh, „Twenty years of attacks on the RSA cryptosystem," *Notices of the American Mathematical Society (AMS)*, vol. LXVI, no. 2, pp. 203-213, 1999.

[619] R. Daniel and L. Brown, *A Weak-Randomizer Attack on RSA-OAEP with e = 3, Eprint*.: International Association for Cryptologic Research, 2005.

[620] J. H. Moore, „Protocol Failures in Cryptosystems," *IEEE Transactions on Information Theory*, no. 5, 1988.

[621] J. H. Moore, „Protocol Failures in Cryptosystems," in *Contemporary Cryptology: The Science of Information Integrity*.: IEEE Press, 1992, pp. 541-558.

[622] International Organization for Standardization, *ISO/IEC 9796, Information Technology – Security Techniques – Digital Signature Sheme Giving Message Recovery*.: ISO, 1991.

[623] Comite Francais d Organisation et de Normalisation Bancaires, *Echanges Telematiques Entre Les Banques et Leurs Clients, Standard ETENAC 5*.: ETEBAC, 1989.

[624] Standards Association of Australia, *Australian Standard 2805.5.3: Electronic Data Transfer – Requirements for Interfaces: Part 5.3 – Data Encipherment Algorithm 2*.: SAA, 1992.

[625] ANSI, *ANSI X9.31, Working Draft: Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry*.: American Bankers Association, 1993.

[626] R.L. Rivest, A. Shamir, and L.M. Adleman, *Cryptographic Communications System and Method, U.S. Patent #4,405,829*., 1983.

[627] CCERT, *CCERT-PUBDOC-2007-02-182, Digitalni potpis*. Zagreb: NCERT, 2007.

[628] L. R. Rivest, A. Shamir, and L. Adleman, „A method for obtaining digital signatures and public-key cryptosystems," *Communication ACM*, vol. XXI, no. 2, pp. 120-126, 1978.

[629] T. ElGamal, „A public key cryptosystem and a signature scheme based on discrete logarithms," in *Advances in Cryptology, volume 196 of Lecture Notes in Computer Science*.: Springer Berlin Heidelberg, 1985, pp. 10-18.

[630] US Department of Commerce, *Digital Signature Standard (DSS), FIPS PUB 186-3*.: Federal Information Processing Standards Publication, 2009.

[631] P. C. Schnorr, „Efficient signature generation by smart cards," *Journal of Cryptology*, vol. IV, pp. 161– 174, 1991.

[632] V. Korać, *Infrastruktura sa javnim ključevima u funkciji zaštite informacionog toka i elektronskog poslovanja*. Beograd: Centar za nove tehnologije, Arheološki insitut, 2010.

[633] D. Cooper et al., *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280*.: RFC Editor, 2008.

[634] International Telecommunications Union ITU, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks – ITU-T Recommendation X.509, Series X: Data networks, open system communications and security directory*.: International Telecommunication Union, 2008.

[635] M. Marković, *Infrastruktura sistema sa tajnim i javnim ključevima, Zbornik radova VJINFO 2001*. Beograd, 2001.

[636] J. Sermersheim, *Lightweight Directory Access Protocol (LDAP): The Protocol, RFC 4511*.: RFC Editor, 2006.

[637] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560*.: RFC Editor, 1999.

[638] H. Beker, J. Friend, and P. Halliden, „Simplifying Key Management in Electronic Funds Transfer Points of Sale Sytems," *Electronics Letters*, vol. XIX, no. 12, pp. 442-444, 1983.

[639] D. E. Denning, „Protecting Public Keys and Signature Keys," *Computer*, vol. XVI, no. 2, pp. 27-35, 1983.

[640] P. Christoffersson et al., *Crypto Users' Handbook: A Guide for Implementors of Cryptographic Protection in Computer Systems*. North Holland: Elsevier Science Publishers, 1988.

[641] C. J. A. Jansen, „On the Key Storage Requirements for Secure Terminals," *Computers and Security*, vol. V, no. 2, pp. 145-149, 1986.

[642] W. Price, *Key Management for Data Encipherment, Security: Proceedings of IFIP/SEC '83*. North Holland: Elsevier Science Publishers, 1983.

[643] G. Pagels-Fick, *Implementation Issues for Master Key Distribution and Protected Keyload Procedures, Computers and Security: A Global Challenge, Proceedings of IFIP/SEC '83*. North Holland: Elsevier Science Publishers, 1984.

[644] D.V. Klein, *Foiling the Cracker': A Survey of, and Implications to, Password Security, Proceedings of the USEN1X UNIX Security Workshop*., 1990.

[645] Bureau of Standards. National, *NBS FIPS PUB 112), Password Usage*.: U.S. Department of Commerce, 1985.

[646] M. R. Needham and D.M. Schroeder, „Using encryption for authentication in large networks of computers," *Communication ACM*, vol. XXI, no. 12, pp. 993–999, 1978.

[647] S.M. Matyas, "Key Handling with Control Vectors," *IBM Systems Journal*, vol. XXX, no. 2, pp. 151- 174, 1991.

[648] S. M. Matyas, A. V. Le, and D.G. Abraham, „A Key Management Scheme Based on Control Vectors," *IBM Systems Journal*, vol. XXX, no. 2, pp. 175-191, 1991.

[649] A. G. Konheim, M.H. Mack, R.K. McNeill, B. Tuckerman, and G. Waldbaum, „The IPS Cryptographic Programs," *IBM Systems Journal*, vol. XIX, no. 2, pp. 253-283, 1980.

[650] C. Asmuth and J. Bloom, „A Modular Approach to Key Safeguarding," *IEEE Transactions on Information Theory*, no. 2, pp. 208-210, 1983.

[651] Verasec. Windows Smart Card Logon – Simple Steps to Setup Windows Smart Card Logon. [Online]. https://versasec.com/downloads/integrators/Windows_SC_Logon_Howto.pdf

[652] RSA Laboratories. PKCS #1: RSA Cryptography Standard. [Online]. https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf

[653] B. Kaliski. PKCS #7: Cryptographic Message Syntax, Version 1.5", RSA Laboratories, East, May 1998. RFC 2315. [Online]. https://tools.ietf.org/html/rfc2315

[654] „PKCS #11 Cryptographic Token Interface Profiles Version 2.40", OASIS standard. [Online]. http://docs.oasis-open.org/pkcs11/pkcs11-profiles/v2.40/os/pkcs11-profiles-v2.40-os.html

Spisak slika

Slika 1. *Hijerarhija podatak–informacija–znanje–mudrost* 16
Slika 2. *Hijerarhija podaci–informacije–znanje–inteligencija–mudrost* 16
Slika 3. *Eksplicitno i implicitno, individualno i organizaciono znanje* 21
Slika 4. *Eksplicitno SECI proces konverzije znanja* 21
Slika 5. *Četiri generičke strategije menadžmenta znanja* 25
Slika 6. *Temeljne komponente menadžmenta znanja* 28
Slika 7. *Dinamična sposobnost kompanije – odnos između menadžmenta znanja i sposobnosti kompanije* 32
Slika 8. *Koncepti povezani sa menadžmentom znanja* 36
Slika 9. *Komponente ljudskog kapitala* 37
Slika 10. *Komponente strukturnog kapitala* 38
Slika 11. *Komponente relacionog (klijentnog) kapitala* 38
Slika 12. *Proces kreiranja znanja* 43
Slika 13. *Klasifikacija sistema za menadžment znanja* 53
Slika 14. *Ključni parametri na koje se fokusira reinženjering* 56
Slika 15. *Kompjuterska podrška fazama procesa odlučivanja u kompaniji* 61
Slika 16. *Interakcija sistema za podršku odlučivanju i informacionih podsistema u kompaniji* 62
Slika 17. *Izvršni sistem za podršku: Integrisanje EIS i DSS* 65
Slika 18. *Učesnici u izgradnji ekspertnog sistema* 66
Slika 19. *Osnovna arhitektura ekspertnih sistema* 67
Slika 20. *Osnovna struktura sistema za upravljanje dokumentima* 69
Slika 21. *Web publikovanje i menadžment dokumentima* 72
Slika 22. *Model učenja* 74
Slika 23. *Proces organizacionog učenja* 76
Slika 24. *Konceptualna arhitektura poslovne inteligencije* 77
Slika 25. *Rudarenje podataka / Data Mining* 80
Slika 26. *Taksonomija rudarenja podataka* 80
Slika 27. *Otkrivanje znanja primenom metoda rudarenja podataka* 82
Slika 28. *Koraci i faze procesa rudarenja podataka* 83
Slika 29. *Odnos analize i relevantnosti atributa nakon izvršavanja pretprocesuiranja podataka* 85
Slika 30. *Upravljanje memorijom organizacije* 98
Slika 31. *Okvir upravljanja memorijom organizacije* 101
Slika 32. *Veza između analitičkog znanja i memorije organizacije* 105
Slika 33. *Arhitektura i mehanizam pretraživanja memorije organizacije* 107
Slika 34. *Veza između materijalizacije memorije organizacije i mogućih tehnika* 108
Slika 35. *Ključne motivacije za „Big Data" analizu* 112
Slika 36. *Koncept ERP sistema* 120
Slika 37. *ERP II idejni model* 122
Slika 38. *Tok podataka u ETL procesu* 129
Slika 39. *ETL proces* 129
Slika 40. *Zvezdasta šema za praćenje grešaka* 131
Slika 41. *Mesto i tok ETL procesa u kreiranju koncepta poslovne inteligencije* 132
Slika 42. *Troslojna arhitektura sa zajedničkim DW i više povezanih „Data Mart"* 133
Slika 43. *Troslojni model sistema skladištenja podataka* 135
Slika 44. *Osnovni model računarstva u oblaku („Cloud Computing")* 139
Slika 45. *Referentna arhitektura računarstva u oblaku* 140

Slika 46. *Primer SaaS provajdera i aplikacija računarstva u oblaku* 141
Slika 47. *Primer „IaaS" provajdera i aplikacija računarstva u oblaku* 141
Slika 48. *Primer „PaaS" provajdera i aplikacija računarstva u oblaku* 142
Slika 49. *Pregled Hadoop okruženja i eko-sistema* 146
Slika 50. *Prikaz Hadoop kernel* 147
Slika 51. *Funkcionisanje virusa* 156
Slika 52. *Prikaz zaustavljanja virusa* 157
Slika 53. *Poruka nakon što je Ransomware zarazio računar ili mrežu korisnika* 160
Slika 54. *Životni ciklus ranjivosti* 162
Slika 55. *CERT sistematizacija i način povezivanja svih faktora u sekvenci ugrožavanja bezbednosti* 164
Slika 56. *Tipičan ciljani napad* 164
Slika 57. *Tradicionalni uzorak aktivnosti napadača* 165
Slika 58. *Prenos i skladištenje ukradenih informacija* 166
Slika 59. *Klasična topologija „firewall"* 173
Slika 60. *Implementacija IDS uređaja u računarskoj mreži* 175
Slika 61. *Slojevita zaštita* 180
Slika 62. *Vremenski prozori proaktivnih i reaktivnih sistema zaštite* 184
Slika 63. *Prošireni vremenski prozor proaktivne zaštite* 186
Slika 64. *Blokovski prikaz simetričnog šifarskog sistema* 191
Slika 65. *Prikaz jedne runde DES algoritma* 193
Slika 66. *Algoritam DES šema* 194
Slika 67. *Funkcija f DES algoritma* 195
Slika 68. *Difie-Hellman razmena ključeva* 204
Slika 69. *Ilustracija postupka asimetričnog šifrovanja* 206
Slika 70. *Ilustracija RSA šifrovanja* 207
Slika 71. *Ilustracija RSA šifrovanja (2)* 210
Slika 72. *Ilustracija matematičke i praktične realizacije RSA algoritma* 212
Slika 73. *Šematski prikaz postupka stvaranja digitalnog potpisa* 215
Slika 74. *Procedura digitalnog poptisivanja i provere potpisa* 216
Slika 75. *Sadržaj digitalnog sertifikata* 217
Slika 76. *Arhitektura predloženog sistema za upravljanje sertifikatima* 226
Slika 77. *Višeslojna arhitektura zaštite komunikacionih kanala u okviru informacionog sistema kompanije* 230
Slika 78. *Arhitektura zaštite komunikacionih kanala u okviru informacionog sistema kompanije na lokalnom nivou* 238
Slika 79. *Format šifrovane poruke* 239
Slika 80. *Arhitektura zaštite komunikacionih kanala u okviru informacionog sistema kompanije korišćenjem Interneta (udaljeni pristup)* 240

Spisak tabela

Tabela 1. *Uporedni prikaz karakteristika tacitnog i eksplicitnog znanja* 19
Tabela 2. *Prošireni popis kategorije znanja sa primerima* 20
Tabela 3. *Elementi lanca znanja sa aktivnostima* 24
Tabela 4. *Strategija menadžmenta znanja* 29
Tabela 5. *Mogući rezultati primene strategije menadžmenta znanja* 29
Tabela 6. *Mogući rezultati primene strategije menadžmenta znanja* 30
Tabela 7. *Kategorije sistema za podršku odlučivanju* 63
Tabela 8. *Osnovne komparativne razlike DSS i ES* 67
Tabela 9. *Razlika između konvencionalnih programa i ekspertnih sistema* 68
Tabela 10. *Aktivnosti i sistemi za menadžment znanja* 71
Tabela 11. *Kancelarijske aktivnosti i IT* 72
Tabela 12. *Pregled definicija „Organizacije koja uči"* 75
Tabela 13. *Primena neuronskih mreža* 89
Tabela 14. *Forme i funkcije memorije organizacije* 95
Tabela 15. *Modeli CommonKADS i tipovi memorije organizacije* 106
Tabela 16. *„Big Data" mogućnosti i njene primarne tehnologije* 113
Tabela 17. *Pregled „Big Data" tehnologija* 115
Tabela 18. *Tehnički i organizacioni faktori koji utiču na primene „Big Data"* 117
Tabela 19. *Zajednički ciljevi proizvođača i korisnika ERP sistema* 126
Tabela 20. *Pregled Razlike između „Data Warehouse" i „Data Mart"* 134
Tabela 21. *Prikaz OLAP arhitektura i njihovih razlika* 137
Tabela 22. *Zajednički primeri pretnji* 149
Tabela 23. *Tabela verovatnoće pretnje* 152
Tabela 24. *Matrica nivoa rizika* (engl. *Risk-Level Matrix*) 152
Tabela 25. *Primer lestvice rizika i aktivnosti koje je potrebno preduzeti* 153
Tabela 26. *Tipični primeri zlonamernog softvera sa osnovnim karakteristikama* 154
Tabela 27. *Matrica stanja za 192-bitni blok* 200
Tabela 28. *Tabela ključa AES algoritma* 200
Tabela 29. *Jačina RSA ključa* 213
Tabela 30. *Preporuka minimalnog simetričnog nivoa i veličine RSA* 213
Tabela 31. *Preporuka minimalnog simetričnog nivoa i veličine RSA* 213

KRIPTOGRAFSKA REŠENJA ZAŠTITE MEMORIJE ORGANIZACIJE SA STANOVIŠTA MENADŽMENTA ZNANJA

ORIGINALITY REPORT

22%

SIMILARITY INDEX

PRIMARY SOURCES

1	www.dragan-pleskonjic.com Internet	1923 words — 2%
2	qdoc.tips Internet	1568 words — 2%
3	www.udg.edu.me Internet	1512 words — 2%
4	nardus.mpn.gov.rs Internet	1023 words — 1%
5	www.agencysnob.com Internet	968 words — 1%
6	es.elfak.ni.ac.rs Internet	701 words — 1%
7	www.scribd.com Internet	633 words — 1%
8	darkomi-it.blogspot.com Internet	595 words — 1%
9	elibrary.matf.bg.ac.rs Internet	564 words — 1%
10	www.adam-europe.eu Internet	523 words — 1%
	hrcak.srce.hr	

11	Internet	492 words — 1%
12	markoslavkovic.com Internet	428 words — < 1%
13	sigurnost.lss.hr Internet	379 words — < 1%
14	people.etf.unsa.ba Internet	329 words — < 1%
15	repozitorij.unios.hr Internet	296 words — < 1%
16	vtsnis.edu.rs Internet	292 words — < 1%
17	www.seminarski-diplomski.rs Internet	286 words — < 1%
18	www.eee-conference.com Internet	253 words — < 1%
19	docplayer.net Internet	244 words — < 1%
20	urn.nsk.hr Internet	215 words — < 1%
21	www.towersnet.rs Internet	211 words — < 1%
22	www.singipedia.singidunum.ac.rs Internet	211 words — < 1%
23	os2.zemris.fer.hr Internet	210 words — < 1%
24	bib.irb.hr Internet	206 words — < 1%

25	alas.matf.bg.ac.rs Internet	205 words —	< 1%
26	inba.info Internet	202 words —	< 1%
27	yuinfo.artkey.rs Internet	202 words —	< 1%
28	www.slideshare.net Internet	201 words —	< 1%
29	www.management.ac.me Internet	198 words —	< 1%
30	repozitorij.svkst.unist.hr Internet	196 words —	< 1%
31	www.cris.uns.ac.rs Internet	180 words —	< 1%
32	repozitorij.unizg.hr Internet	169 words —	< 1%
33	www.ktios.net Internet	166 words —	< 1%
34	www.infotech.org.rs Internet	153 words —	< 1%
35	moam.info Internet	146 words —	< 1%
36	issuu.com Internet	140 words —	< 1%
37	www.infoteh.rs.ba Internet	138 words —	< 1%
38	www.eknfak.ni.ac.rs Internet	138 words —	< 1%

39	univerzitetpim.com Internet	137 words — < 1%
40	es.scribd.com Internet	131 words — < 1%
41	www.cip.unze.ba Internet	127 words — < 1%
42	www.hakom.hr Internet	122 words — < 1%
43	docshare.tips Internet	113 words — < 1%
44	www.bak.hr Internet	109 words — < 1%
45	spvp.zesoi.fer.hr Internet	108 words — < 1%
46	documents.mx Internet	108 words — < 1%
47	www.emc-review.com Internet	108 words — < 1%
48	www.fon.bg.ac.rs Internet	106 words — < 1%
49	pt.scribd.com Internet	103 words — < 1%
50	www.meste.org Internet	93 words — < 1%
51	symorg.fon.bg.ac.rs Internet	93 words — < 1%
52	uvidok.rcub.bg.ac.rs Internet	91 words — < 1%

53	vts.edu.rs Internet	84 words — < 1%
54	www.ftn.kg.ac.rs Internet	81 words — < 1%
55	www.crnarupa.singidunum.ac.rs Internet	81 words — < 1%
56	bs.scribd.com Internet	77 words — < 1%
57	link-university.com Internet	76 words — < 1%
58	www.vps.ns.ac.rs Internet	76 words — < 1%
59	www.mkt.gov.ba Internet	74 words — < 1%
60	eteze.bg.ac.rs Internet	72 words — < 1%
61	dragan-pleskonjic.com Internet	71 words — < 1%
62	ddfe.curtin.edu.au Internet	68 words — < 1%
63	zir.nsk.hr Internet	66 words — < 1%
64	www.skladistenje.com Internet	65 words — < 1%
65	2009.telfor.rs Internet	64 words — < 1%
66	Marija Marković-Blagojević, Đorđe Ilić, Dijana	64 words — < 1%

Petkov. "Business in the cloud application management of information systems", Trendovi u poslovanju, 2014
Crossref

67	www.gov.me Internet	61 words — < 1%
68	www.ubs-asb.com Internet	60 words — < 1%
69	eubd.edu.ba Internet	54 words — < 1%
70	www.inf.uniri.hr Internet	54 words — < 1%
71	www.vtsnis.edu.rs Internet	52 words — < 1%
72	edoc.pub Internet	50 words — < 1%
73	www.cert.hr Internet	50 words — < 1%
74	documents.tips Internet	50 words — < 1%
75	www.dmi.uns.ac.rs Internet	49 words — < 1%
76	www.fonforum.org Internet	49 words — < 1%
77	www.itvestak.org.rs Internet	48 words — < 1%
78	idoc.pub Internet	46 words — < 1%
79	www.vtg.mod.gov.rs Internet	44 words — < 1%

80	eteze.arts.bg.ac.rs Internet	43 words — < 1%
81	galilej.com Internet	41 words — < 1%
82	www.goranklepac.com Internet	41 words — < 1%
83	www.mathos.unios.hr Internet	37 words — < 1%
84	www.zastita.ac.me Internet	37 words — < 1%
85	www.cis.hr Internet	36 words — < 1%
86	repozitorij.fsb.unizg.hr Internet	36 words — < 1%
87	147.91.175.145 Internet	36 words — < 1%
88	www.singipedia.com Internet	36 words — < 1%
89	infoteh.etf.ues.rs.ba Internet	34 words — < 1%
90	darhiv.ffzg.unizg.hr Internet	34 words — < 1%
91	indel.etfbl.net Internet	33 words — < 1%
92	wip.viser.edu.rs Internet	33 words — < 1%
93	repository.fthm.uniri.hr	

	Internet	33 words — < 1 %
94	www.jonik.rs Internet	33 words — < 1%
95	fr.scribd.com Internet	30 words — < 1%
96	tims.rs Internet	30 words — < 1%
97	unidocs.rs Internet	30 words — < 1%
98	www.maturskiradovi.net Internet	29 words — < 1%
99	predmet.singidunum.ac.rs Internet	28 words — < 1%
100	www.vtmsts.edu.rs Internet	28 words — < 1%
101	Miroslav Terzic. "Proposal for an ad hoc computer network in the military electronic systems department at the military academy applying bluetooth technology", Vojnotehnicki glasnik, 2011 Crossref	26 words — < 1%
102	www.vidipedija.com Internet	24 words — < 1%
103	lis.irb.hr Internet	24 words — < 1%
104	www.fpspo.edu.rs Internet	22 words — < 1%
105	www.seminarski-diplomski.co.rs	

Internet

22 words — < 1%

106	www.fpmoz.ba Internet	21 words — < 1%
107	www.pfst.hr Internet	21 words — < 1%
108	sema.rs Internet	21 words — < 1%
109	www.tfzr.uns.ac.rs Internet	20 words — < 1%
110	www.masfak.ni.ac.rs Internet	19 words — < 1%
111	bisec.rs Internet	18 words — < 1%
112	www.european-safety-engineer.org Internet	18 words — < 1%
113	fer.hr Internet	17 words — < 1%
114	docplayer.org Internet	16 words — < 1%
115	www.eventiotic.com Internet	16 words — < 1%
116	www.puskice.org Internet	16 words — < 1%
117	docslide.us Internet	16 words — < 1%

Predrag Pravdić, Marija Marković-Blagojević. "Menadžment

118	procesima u savremenom poslovanju", Trendovi u poslovanju, 2013 Crossref	16 words — < 1%
119	docplayer.fi Internet	15 words — < 1%
120	poslovna-inteligencija.blogspot.com Internet	14 words — < 1%
121	www.mitjatanjga.org Internet	14 words — < 1%
122	ttl.masfak.ni.ac.rs Internet	13 words — < 1%
123	www.vtssa.edu.rs Internet	13 words — < 1%
124	repozitorij.efzg.unizg.hr Internet	12 words — < 1%
125	mf.unibl.org Internet	12 words — < 1%
126	www.ibm.com Internet	11 words — < 1%
127	specinf.tvz.hr Internet	11 words — < 1%
128	ess.ekof.bg.ac.rs Internet	11 words — < 1%
129	www.bpa.edu.rs Internet	11 words — < 1%
130	dku.hr Internet	10 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	< 15 WORDS
EXCLUDE BIBLIOGRAPHY	ON		