INFORMACIONI SISTEMI U FUNKCIJI REVIZIJE

PRIRUČNIK

Prof. dr Ljiljana Kašćelan

Podgorica, januar 2026. godine

Prof. dr Ljiljana Kašćelan

PRIRUČNIK

INFORMACIONI SISTEMI U FUNKCIJI REVIZIJE

LITERATURA ZA POLAGANJE ISPITA ZA DRŽAVNOG REVIZORA

PODGORICA, JANUAR 2026. GODINE

Autor

Prof. dr Ljiljana Kašćelan

prvo izdanje

Izdavač

Državna revizorska institucija Crne Gore

Recenzent

dr Sunčica Vuković

Lektor

Katarina Milonjić

Tiraž

25 primjeraka

Štampa

Golbi DOO, Podgorica

CIP – Katalogizacija u publikaciji Nacionalna biblioteka Crne Gore, Cetinje

ISBN 978-9940-752-10-1
COBISS.CG-ID 36787204

Recenzija

Priručnik *Informacioni sistemi u funkciji revizije* prof. dr. Ljiljane Kašćelan predstavlja izuzetno vrijedan i savremeno koncipiran udžbenički materijal koji povezuje teorijske osnove informacionih sistema sa njihovom praktičnom primjenom u revizorskom radu. Autor na jasan, metodološki dosljedan i pedagoški pristupačan način uvodi čitaoca u kompleksan svijet informacionih tehnologija, baza podataka i digitalnih alata koji čine osnovu savremene revizorske profesije.

Knjiga je podijeljena u sedam cjelina koje prate logičan razvoj od temeljnih pojmova informacionih sistema, preko tehničke i softverske infrastrukture, do konkretne primjene specijalizovanih alata za reviziju. Takva struktura omogućava postepeno usvajanje znanja – od razumijevanja koncepata, preko tehničkog funkcionisanja sistema, do praktične upotrebe u profesionalnom okruženju.

Prvo poglavlje obrađuje osnovne pojmove informacionih sistema i njihovu ulogu u savremenim organizacijama, posebno u kontekstu državne i finansijske revizije. Objašnjenja su prilagođena i čitaocima bez tehničke pozadine, čime se postiže balans između teorijske preciznosti i pristupačnosti. Autor jasno razdvaja informacione tehnologije od informacionih sistema, ističući njihovu komplementarnost i značaj za efikasnost poslovnih procesa.

Drugo poglavlje posvećeno je bazama podataka i modelima njihove organizacije. Posebna vrijednost ovog dijela jeste objašnjenje relacione strukture podataka i koncepta integriteta baze, uz praktične primjere koji pokazuju kako se podaci koriste u revizorskim analizama. Obrađene su i savremene koncepcije poput Big Data i Cloud computing-a, čime autor unosi aktuelnu dimenziju u tradicionalne koncepte upravljanja podacima.

U trećem i četvrtom poglavlju predstavljeni su sistemi za elektronsko upravljanje dokumentacijom (eDMS) i web-portali kao alati za komunikaciju i distribuciju informacija u revizorskim institucijama. Ovi djelovi pružaju čitaocu razumijevanje kako digitalizacija administrativnih procesa doprinosi transparentnosti i efikasnosti u radu javnih i privatnih organizacija.

Peto i šesto poglavlje objašnjavaju ulogu internet tehnologija i aplikativnog softvera (Word, Excel, Outlook, PowerPoint) u svakodnevnom revizorskom radu. Pristup je praktičan, a primjeri su usmjereni ka stvarnim poslovnim situacijama – od pripreme izvještaja i analiza do komunikacije sa klijentima. Na taj način priručnik ne ostaje na nivou teorijskog pregleda, već služi i kao praktični vodič.

Najopsežnije i najvažnije, sedmo poglavlje posvećeno je specijalizovanom softveru za analizu podataka – CaseWare IDEA. Ovaj dio priručnika posebno se izdvaja jer čitaocu daje detaljno, korak-po-korak uputstvo za rad u profesionalnom alatu koji je standard u revizorskoj praksi. Autor prikazuje sve faze analize: kreiranje projekata, uvoz i formatiranje podataka, definisanje kriterijuma, analitičke procedure poput sumarizacije, detekcije praznina, spajanja i poređenja baza, kao i izvoz rezultata u Excel i PDF formate. Didaktička vrijednost ovog dijela ogleda se u sistematičnoj strukturi, jasno formulisanim uputstvima i upotrebi terminologije prilagođene početnicima, ali je i korisna za napredne studente i praktičare.

Autor koristi izbalansiran metodološki pristup koji kombinuje teorijsko objašnjenje, ilustrativne primjere i konkretna uputstva. Svaka tema razvija se od osnovnog pojma do praktične primjene, uz naglasak na razumijevanje funkcionalnih odnosa između tehnologije i revizije. Jezik je jasan, precizan i terminološki dosljedan, što doprinosi naučnoj validnosti i pedagoškoj vrijednosti teksta.

Posebno treba istaći pažljivo uvedene tehničke termine na crnogorskom jeziku, uz zadržavanje engleskih izraza u zagradama tamo gdje je to neophodno zbog stručne prepoznatljivosti. Time se postiže ravnoteža između lokalne terminologije i međunarodnih standarda u oblasti informatičke revizije.

Priručnik se može koristiti u više konteksta: kao udžbenik za studente, kao priručnik za obuku revizora i internih kontrolora, te kao referentni vodič za praktičare koji žele produbiti razumijevanje o analizi podataka. Posebna prednost je kombinacija teorijskih poglavlja i praktičnih uputstava za rad u IDEA softveru – što je rijetko objedinjeno u jednom djelu.

Primjeri iz prakse, poput uvida u spajanje baza faktura i isplata radi otkrivanja neusaglašenih transakcija, pokazuju kako informacione tehnologije postaju alat u otkrivanju nepravilnosti i jačanju integriteta finansijskog izvještavanja. Autor na taj način uspješno prevodi apstraktne koncepte u konkretne revizorske procedure.

Knjiga doprinosi razvoju literature u oblasti informacione tehnologije u funkciji revizije, koja je u crnogorskom i regionalnom prostoru još uvijek nedovoljno zastupljena. Originalnost se ogleda u integraciji oblasti koje se tradicionalno obrađuju odvojeno – informacioni sistemi, baze podataka, internet tehnologije i revizorski softver. Ova sinteza omogućava da čitalac dobije cjelovitu sliku o digitalnom okruženju u kojem djeluje savremeni revizor.

Autorka uspješno spaja akademski pristup sa praktičnom perspektivom čime priručnik prevazilazi ulogu udžbenika i postaje most između teorije i profesionalne prakse. Kroz jasno objašnjenje načina na koji informacione tehnologije podržavaju revizorsku metodologiju, knjiga istovremeno osnažuje kompetencije budućih revizora i podstiče razvoj digitalnih vještina u finansijskom nadzoru.

Priručnik *Informacioni sistemi u funkciji revizije* predstavlja savremen, sveobuhvatan i izuzetno koristan izvor znanja za sve koji se bave revizijom, kontrolom i analizom podataka. Spoj teorijskog utemeljenja, praktičnih primjera i preciznih uputstava čini ga ne samo edukativnim, već i primjenljivim u svakodnevnom radu revizora. Struktura, jezik i vizuelna organizacija teksta svjedoče o pažljivoj didaktičkoj obradi i profesionalnom iskustvu autorke.

Zahvaljujući ovom priručniku, revizori, studenti i istraživači dobijaju jasno vođen put kroz tehnološke aspekte revizije – od razumijevanja informacionih sistema do primjene naprednih analitičkih alata. Time se značajno doprinosi modernizaciji obrazovanja i prakse revizije u digitalnom dobu.

Podgorica, 29. 10. 2025.

Dr Sunčica Vuković



Sadržaj

1. Informacioni sistemi 6
   1.1. Pojam informacionog sistema 6
   1.2. Struktura informacionog sistema 6
   1.3. Vrste informacionih sistema 47
   1.4. Informacioni sistemi i moderne tehnološke platforme 48
2. Baze podataka 58
   2.1. Relacioni model 58
   2.2. Big data 61
   2.3. Cloud computing 62
3. Elektronski sistemi za upravljanje dokumentima (eDMS) 64
4. E-portal 66
5. Internet tehnologije kao podrška revizorskom poslovanju 73
   5.1. Uvod u internet i web-tehnologiju 73
   5.2. Web-portal 74
   5.3. Web-pregledači 75
   5.4. Internet podržana revizija 76
6. Aplikativni softver kao podrška revizorskom poslovanju 78
   6.1. MS Word – tekst procesor u funkciji revizijske dokumentacije 78
   6.2. MS Excel 79
   6.3. MS Outlook 82
   6.4. MS PowerPoint 84
7. Specijalizovani softver za reviziju – IDEA softver za analizu podataka 86
   7.1. Opšte informacije 86
   7.2. Glavne karakteristike 87
   7.3. Ispitivanja 90
   7.4. Podaci 91
   7.5. Analiza 96
   Literatura 110

1. Informacioni sistemi

1.1. Pojam informacionog sistema

Informacioni sistem predstavlja kombinaciju aktivnosti, tehnologija i ljudi koji zajedno omogućavaju prikupljanje, obradu, čuvanje, distribuciju i korišćenje informacija. Ovaj sistem podržava donosioce odluka u organizacijama tako što pretvara sirove podatke u korisne informacije. U kontekstu državne revizije, informacioni sistem pomaže u praćenju javnih finansija, upravljanju rizicima i osiguranju transparentnosti. Ovo znači da se pomoću njih analiziraju tokovi novca u budžetu, identifikuju moguće prevare ili gubici, te osigurava da su finansijski podaci javno dostupni i razumljivi, čime se gradi povjerenje u rad javnih institucija. Na primjer, revizori pristupaju sistemu da provjere kako se budžetska sredstva raspoređuju, ima li nepravilnosti poput nepotrebnih troškova i da li se izvještaji objavljuju na način koji građani mogu razumjeti, čime se promoviše odgovornost javnih tijela.

Informacioni sistem se razlikuje od informacionih tehnologija. Informacione tehnologije obuhvataju fizičke uređaje, programe i komunikacione mreže koji služe za obradu podataka. Informacioni sistem uključuje i ljude, procese i strategije koji daju smisao tim tehnologijama. Na primjer, informacioni sistem u Ministarstvu finansija prikuplja podatke o porezima, obrađuje ih da bi izračunao dugovanja i distribuira obavještenja građanima.

Informacioni sistem igra ključnu ulogu u reviziji jer omogućava procjenu efikasnosti i sigurnosti poslovanja organizacije. Revizori koriste taj sistem da bi analizirali kako organizacija prikuplja, obrađuje i čuva podatke, utvrđujući da li su procesi brzi, tačni i zaštićeni od rizika. Na primjer, u Ministarstvu finansija revizori pregledaju informacioni sistem za naplatu poreza da bi provjerili da li pravilno izračunava dugovanja i osigurava zaštitu ličnih podataka građanima. Ako sistem ima slabosti, poput neefikasne obrade ili ranjivosti na napade, revizori predlažu poboljšanja da bi se osigurala ekonomičnost i pouzdanost.

Organizacije zavise od ovih sistema za digitalizaciju usluga, što povećava rizike poput sajber napada ili gubitka podataka. Revizori analiziraju kako informacioni sistem podržava misiju organizacije, osiguravajući da bude ekonomičan i siguran. Pored toga, revizori koriste sopstvene alate za podršku procesu revizije, poput programa za analizu podataka ili dokumentaciju nalaza, ali glavni fokus ostaje na informacionom sistemu revidirane organizacije.

1.2. Struktura informacionog sistema

Informacioni sistem sastoji se od više međusobno povezanih komponenti koje zajedno osiguravaju njegovo funkcionisanje. Ova struktura omogućava efikasnu obradu informacija u organizacijama, uključujući javni sektor. U kontekstu revizije, razumijevanje strukture pomaže revizorima da identifikuju slabosti i procijene rizike. Komponente se mogu podijeliti na hardver (hardware), softver (software), mreže (netware), baze podataka (databases) i organizacione elemente (orgware) koji uključuju ljude i procese.

Hardver

Hardver čine fizičke komponente informacionog sistema, u prvom redu računari. Računar predstavlja mnogo više od skupa elektronskih uređaja koji procesiraju informacije. Računar je sistem, tj. kombinacija međusobno povezanih komponenti koje obavljaju osnovne funkcije ulaza, procesiranja, izlaza, memorisanja i kontrole, obezbjeđujući na taj način korisniku moćan alat za obradu informacija. Za uspješno korišćenje i upravljanje računarom od ključnog značaja jeste shvatanje računara kao računarskog sistema. Na ovaj način računar se može zamisliti kao najmanji mikroračunarski uređaj, ali i kao velika računarska mreža čije su komponente međusobno povezane telekomunikacionim mrežnim linkovima unutar jednog kompleksa zgrada ili čak šireg geografskog područja.

Slika 1. prikazuje da je računar sistem hardverskih uređaja organizovanih prema sljedećim funkcijama sistema (Kašćelan, 2016):

Ulaz (Input) – U ulazne uređaje računarskog sistema spadaju tastatura, dodirni ekrani (touch screen), olovke, elektronski miš, optički skener i slično. Oni konvertuju podatke u elektronsku formu, bilo da su dobijeni kroz direktni unos ili preko računarske mreže.

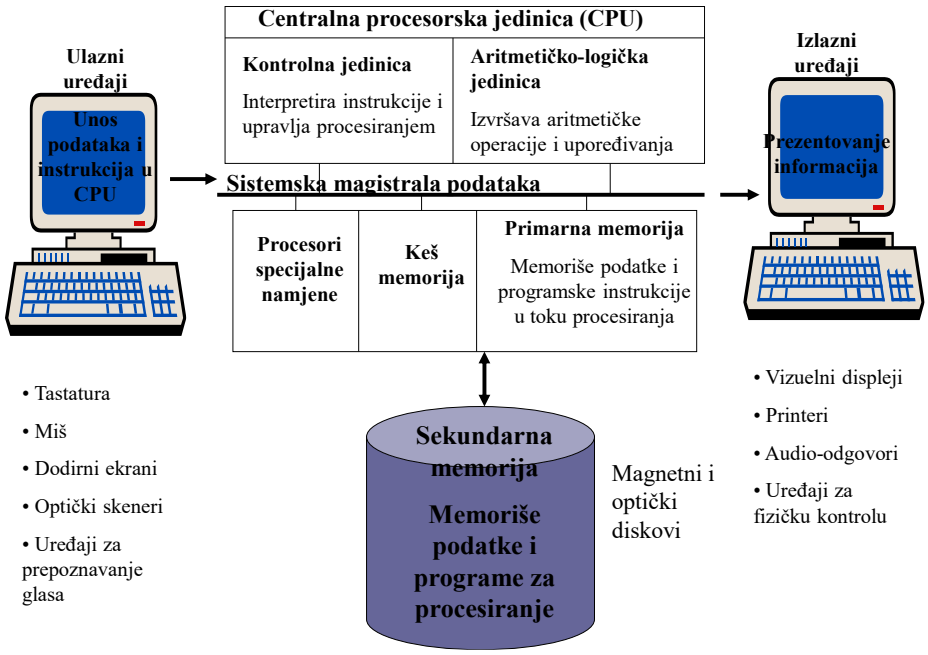
Obrada (Processing) – Centralna procesorska jedinica (Central Processing Unit – CPU) jeste glavna komponenta za obradu podataka u računarskom sistemu. Kod mikroračunara ova jedinica se naziva mikroprocesor. Konceptualno, CPU se može podijeliti u dvije glavne komponente, a to su aritmetičko-logička jedinica i kontrolna jedinica. Elektronsko kolo aritmetičko-logičke jedinice izvršava aritmetičke i logičke funkcije koje su potrebne prilikom izvršavanja softverskih instrukcija. CPU sadrži i registre i keš memoriju, koji predstavljaju veoma brzu i privremenu memoriju za instrukcije i podatke. Takođe, može sadržati i neke pomoćne procesore specijalne namjene.

Izlaz (Output) – Izlazni uređaji računarskog sistema obuhvataju monitore (uređaje sa video-displejom), štampače (printere), audio izlazne uređaje i slično. Oni konvertuju elektronske informacije generisane računarskim sistemom u format pogodan za prezentovanje korisniku.

Memorisanje (Storage) – Uređaj koji memoriše (čuva) podatke i softverske instrukcije u toku obrade jeste primarna memorijska jedinica, koja se naziva radna (operativna) memorija. Računarski sistem osim primarne memorije ima i sekundarne memorijske uređaje, kao što su magnetni ili optički diskovi. Oni trajno memorišu podatke i programe koji se obrađuju na računaru.

Kontrola – Kontrolna jedinica centralne procesorske jedinice je kontrolna komponenta računarskog sistema. Ovo elektronsko kolo interpretira softverske instrukcije i u skladu sa tim upućuje odgovarajuće komande svim komponentama računarskog sistema.

Brzina procesiranja – Brzina procesiranja govori nam koliko je brz računarski sistem, tj. koliko brzo obrađuje instrukcije. Nekada se brzina računara mjerila milisekundama (hiljaditi dio sekunde) ili mikrosekundama (milioniti dio sekunde). Danas računari rade u rangu nanosekundi (bilioniti dio sekunde), pa čak i pikosekundi (trilioniti dio sekunde). Ove brzine su gotovo neshvatljive. Kolika je to brzina, najbolje može ilustrovati sljedeći primjer: kada bi se pravio po jedan korak svake nanosekunde, Zemlja bi se obišla 20 puta u toku jedne sekunde.



Slika 1. Koncept računarskog sistema

Brzina računara može se izraziti i brojem obavljenih operacija u sekundi. Superkompjuteri mogu imati brzinu od jednog triliona operacija po sekundi (teraflop). Međutim, većina računara danas ima brzinu procesiranja programskih instrukcija izraženu u milijardama instrukcija po sekundi (GIPS – giga instrukcija po sekundi).

Za mjerenje brzine računarskog sistema koriste se i druge jedinice, kao što su gigaherci (GHz), tj. milijardu ciklusa po sekundi. Ovdje je riječ o vremenskim ciklusima mikroprocesora zasnovanim na internom časovniku. Zato se ova brzina često zove i clock speed mikroprocesora.

Međutim, ovako izražene brzine računarskog sistema mogu biti i nedovoljno tačni indikatori stvarne brzine procesiranja mikroprocesora. Naime, brzina procesiranja zavisi i od mnoštva drugih faktora, kao što su: dužina ciklusa, magistrala koja povezuje mikroprocesorske komponente, kapacitet registara za procesiranje instrukcija, korišćenje ultra brze keš memorije ili specijalizovanih pomoćnih procesora, kakav je npr. matematički koprocesor za brza aritmetička izračunavanja i drugo.

Podaci se u kompjuterskom sistemu memorišu i obrađuju u binarnom brojnom sistemu (sistem koji se sastoji od dvije cifre 0 i 1). Ovakav način prezentovanja podataka potiče od svojstava memorijskih medijuma koji mogu da se nađu u dva stanja. Kod poluprovodničkih memorija riječ je o provodnom i neprovodnom stanju, dok se kod magnetnih memorija ova dva stanja ogledaju u mogućnosti polarizovanja magnetnog polja na pozitivno i negativno.

Dakle, binarne karakteristike memorijskih medijuma jesu osnovni razlog što je binarni sistem osnov za prezentovanje podataka u računaru. Stoga provodno stanje predstavlja binarnu jedinicu

za elektronska kola, dok neprovodno stanje predstavlja binarnu nulu. Za magnetne medijume, magnetno polje namagnetisane tačke u jednom pravcu predstavlja binarnu jedinicu, a u drugom pravcu – binarnu nulu.

Najmanji dio podatka naziva se bit i predstavlja jednu jedinicu ili nulu. Kapacitet memorije se izražava bitima. Osnovna jedinica podataka sa kojom kompjuter radi jeste bajt (B) i predstavlja binarni kôd jednog karaktera (karakter je slovo, cifra ili specijalni znak). Postoji više standarda za kodiranje karaktera. Opšteprihvaćeni standard jeste ASCII (američki standardni kôd za unutrašnju razmjenu informacija), kod koga se svaki karakter kodira sa 8 bita. U Tabeli 1 predstavljeni su ASCII kodovi nekih karaktera (Kašćelan, 2016). Većina računara koristi ASCII kodove, pa se može zaključiti da jedan bajt ima 8 bita. S obzirom na to da su danas memorijski medijumi velikih kapaciteta, za mjerenje kapaciteta koriste se i veće jedinice, kao što su kilobajt (KB), megabajt (MB), gigabajt (GB) i terabajt (TB). Iako kilo u metričkom sistemu znači hiljadu, kompjuterska industrija koristi K da predstavi 1024, odnosno 210 karaktera. Tako na primjer 10 MB predstavlja stvarnih 10485760, a ne 10 miliona karaktera. Ove razlike se često ignorišu zbog jednostavnijeg opisa memorijskih kapaciteta. Tako megabajt ima oko milion bajta memorije, gigabajt – oko bilion, a terabajt – oko trilion bajta.

Tabela 1. Primjeri ASCII kodova

Karakter	ASCII kod
0	00110000
1	00110001
2	00110010
3	00110011
...	...
A	01000001
B	01000010
C	01000011
...	...

Primarna memorija računara sastoji se od poluprovodničkih memorijskih čipova. To je radna memorija u kojoj kompjuter smješta podatke i instrukcije u toku obrade.

Glavna prednost poluprovodničke memorije je velika brzina pristupa podacima. Glavni nedostatak poluprovodničke memorije je nepostojanost – volatilnost, tj. ukoliko nema neprekidnog strujnog napajanja, sadržaj iz nje se briše. Ovaj problem se prevazilazi upotrebom baterijskog napajanja ili generatora struje. Alternativno rješenje jeste stalno presnimavanje sadržaja iz operativne memorije na neki trajni memorijski medijum i, u slučaju nestanka struje, ponovno vraćanje u radnu memoriju. Kapacitet primarne (poluprovodničke) memorije se danas najčešće mjeri desetinama GB.

Operativna memorija sastavljena je od dva osnovna tipa memorije, tj. dijelom je RAM, a dijelom ROM (Read Only Memory).

RAM – Random Access Memory: RAM memorijski čipovi čine većinu operativne memorije. Svakoj memorijskoj lokaciji može se pristupiti (čitati) i promijeniti (pisati), pa se ove memorije nazivaju i čitaj-piši memorije. Ova vrsta memorije je nepostojana (volatilna).

ROM – Read Only Memory: Postojani memorijski čipovi za trajno memorisanje takođe su sastavni dio operativne memorije. ROM jeste memorija samo za čitanje, ne može se brisati niti presnimavati. Obično su u njoj smještene najčešće korišćene kontrolne instrukcije kod kontrolne jedinice, kao i inicijalni dio operativnog sistema (BIOS) kod operativne memorije. Ovi sadržaji nasnimljeni su u toku proizvodnje računara i ne mogu se mijenjati.

Sekundarna memorija računara je najčešće magnetna memorija u vidu hard diska. Hard disk je fiksiran u kućištu računara. Sastoji se od više magnetnih diskova na vertikalnoj osovini, a između njih se nalaze R/W glave. Kapacitet im se kreće od nekoliko stotina GB do nekoliko desetina TB.

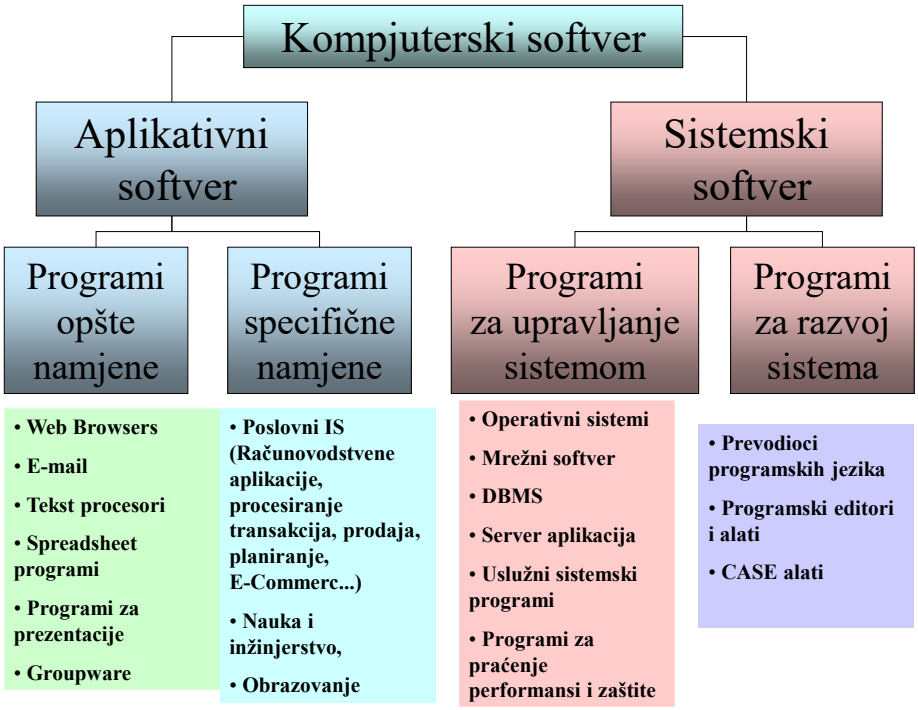
Danas se sekundarna memorija sve češće pojavljuje i u vidu SSD (Solid State Drive). Zahvaljujući elektronskom principu rada, SSD omogućava znatno brže čitanje i pisanje podataka, tiši je, troši manje energije i otporniji je na udarce. S druge strane, hard disk pruža veći kapacitet po nižoj cijeni, ali je sporiji i podložan mehaničkim oštećenjima.

Pojavljuje se i u vidu optičke memorije tj. optičkih diskova (Compact Disk – CD). Optički disk je metalni disk na kome se podaci snimaju laserski tako što se prave mikroskopska udubljenja na spiralnim trakama na površini diska. Laserski uređaj čita binarne kodove podataka prezentovane tim udubljenjima, tj. odgovarajućom refleksijom svjetlosti koju emituju ta udubljenja. Ovi diskovi memorišu podatke gustinom mnogo većom nego magnetni diskovi, ali imaju manju brzinu upisivanja podataka, i skuplji su. Koriste se najviše za image i multimedijalne podatke (katalozi, prezentacije, enciklopedije itd.).

USB flash memorije su vrsta prenosive sekundarne memorije koja koristi flash tehnologiju zasnovanu na EEPROM principu (Electrically Erasable Programmable Read-Only Memory), što znači da se može elektronski brisati i ponovo programirati. Za razliku od klasičnog EEPROM-a u okviru primarne memorije, kod kojeg se podaci brišu i upisuju na nivou bajta, flash memorija obavlja ove operacije na nivou većih blokova, što omogućava znatno veću brzinu rada. Iako su pouzdane i praktične, imaju ograničen broj ciklusa upisa i brisanja (otprilike do 100.000 puta), a zbog načina upravljanja blokovima dio memorijskog prostora može postati neiskoristiv tokom vremena, što utiče na efektivni kapacitet i dugotrajnost uređaja.

Softver

Softver predstavlja skup programa koji se izvršavaju na računaru. Slika 2 prikazuje osnovne tipove i funkcije aplikativnog i sistemskog softvera (Kašćelan, 2016). Aplikativni softver predstavlja programe namijenjene za rješavanje konkretnih problema, aktivnosti i zadataka korisnika računarskog sistema. Sistemski softver čini klasu programa koja obezbjeđuje efikasno funkcionisanje računarskog sistema i koordiniranje aktivnosti hardverskih resursa u zavisnosti od zahtjeva aplikativnog softvera. Sistemski softver predstavlja međusloj, tj. vezu između hardvera i aplikativnog softvera.



Slika 2. Podjela kompjuterskog softvera

Slika 2 prikazuje da **aplikativni softver** podrazumijeva skup programa koji se mogu podijeliti na programe opšte namjene i programe specifične namjene.

Na tržištu postoje hiljade različitih softverskih **paketa specifične namjene** koji podržavaju poslovne i druge aktivnosti korisnika. Na primjer, poslovni paketi podržavaju upravljačke i operativne aktivnosti kao što su procesiranje transakcija, podrška odlučivanju, upravljanje prodajom, analiza investicija i elektronska trgovina. Softver specifične namjene u oblasti nauke i inženjerstva ima glavnu ulogu u istraživačkim i razvojnim programima, u dizajniranju i proizvodnji visokokvalitetnih proizvoda i dr. Tu su takođe paketi namijenjeni obrazovanju, zabavi i sl.

Informacioni sistemi predstavljaju integrisanu kombinaciju kros-funkcionalnih softvera koji pokrivaju više poslovnih funkcija.

Glavni kros-funkcionalni poslovni softveri su:

- **ERP (Enterprise Resource Planing)** – softveri za planiranje i upravljanje resursima (finansijskim, ljudskim, materijalnim i dr.);
- **CRM (Customer Relationship Management)** – softveri za odnose sa korisnicima;
- **SCM (Supply Chain Management)** – softveri koji omogućavaju elektronsko poslovanje sa dobavljačima, distributerima i prodavcima koji čine aktere u lancima nabavke.

Istorijski ERP sistemi nastali su od sistema za planiranje materijalnih i proizvodnih resursa MRP (Material Requirements Planning). Danas ERP sistemi automatizuju i integrišu poslovne procese u proizvodnji (planiranje proizvodnje, logistika, prodaja, zalihe, narudžbe, distribucija), u finansijama i računovodstvu, kao i u upravljanju ljudskim resursima (back-office). Extended

(prošireni) ERP sistemi danas obuhvataju i CRM i SCM sisteme, kao i sisteme poslovne inteligencije (Bbusiness Intelligence – BI) i e-poslovanja, i tako čine univerzalni kros-funkcionalni softver koji se koristi u poslovanju. Ovakvi sistemi, osim unutrašnjeg, obuhvataju i spoljašnje poslovanje. Extended ERP sistemi su obično gotovi standardizovani softverski paketi koji se pomoću parametara prilagođavaju pojedinačnoj organizaciji. Najpoznatiji prošireni ERP paketi na tržištu su SAP (Systems Applications and Products), Microsoft Dynamics 365 i ORACLE – People Soft.

Programi opšte namjene izvršavaju poslove standardnog procesiranja informacija za krajnje korisnike, kao što su na primjer obrada teksta, obrada tabela, izrada prezentacija i drugo. Oni značajno povećavaju produktivnost krajnjih korisnika. Oni takođe uključuju i programe koji podržavaju komunikacije i saradnju između radnih grupa i timova, kao što su web browseri, e-mail programi i groupware programi.

Programi opšte namjene su obično integrisani u pakete i poznati su pod nazivom integrisani paketi. Na tržištu postoje ovakvi integrisani paketi koje nude različiti proizvođači (najpoznatiji je Microsoft Office). Najpoznatiji programi u okviru **MS Office** paketa su **Word (obrada teksta)**, **Excel (obrada tabela)**, **Outlook (e-mail procesori)** i **PowerPoint (izrada prezentacija)**.

Cijena integrisanog paketa znatno je manja od ukupne cijene pojedinačnih softverskih paketa. Svi programi koji čine integrisani paket imaju sličan GUI (ikone, toolbar i statusbar, menije i slično) koji daje isti izgled i osjećaj za rad i čini ih jednostavnijim za savladavanje i upotrebu. Programi u okviru integrisanog paketa imaju standardne alate kao što su help wizard i drugo. Njihova velika prednost jeste i mogućnost kopiranja i prenošenja djelova fajlova iz jednog u drugi, kao i međusobno importovanje fajlova.

Web Browseri (internet pregledači) su gotovo najvažniji programi opšte namjene za mnoge korisnike. Browser programi, kao što su Google Chrome i Microsoft Edge, predstavljaju ključni softverski interfejs koji koristimo za point and click putovanje po hiperlinkovanim web-resursima na internetu, ali i na intranet mrežama (mrežama unutar preduzeća).

Iako su proizvedeni radi surfovanja po internetu, može se reći da danas browseri postaju univerzalna softverska platforma za pretraživanje informacija, za elektronsku poštu, transfer multimedijalnih fajlova, učešće u diskusionim grupama i za još mnogo drugih internet i intranet primjena. Tako, ukoliko želite da gledate video-film, telefonirate, downloadujete neki softver, održite video-konferenciju sa poslovnim partnerima ili svojim zaposlenima, da provjerite vaš e-mail, pregledate cjenovnik vaših proizvoda ili plan rada projektnog tima, ili da upotrijebite neki program koji podržava upravljanje i operativnost u organizaciji (npr. da pregledate izvještaj o prodaji, da pošaljete narudžbenicu dobavljaču itd.) – vi ćete to uraditi pomoću Web Browser-a. Dakle, Web Browser je univerzalni klijent, tj. univerzalni softver koji se instalira na klijentima intranet mreže.

E-mail procesori takođe predstavljaju veoma važne softvere opšte namjene. Prva stvar koju mnogi zaposleni širom svijeta svaki radni dan urade, jeste da provjere svoj e-mail. Elektronska pošta je promijenila način na koji ljudi rade i komuniciraju. Milioni korisnika sada koriste e-mail softver da bi ostvarili komunikaciju slanjem i primanjem elektronskih poruka preko interneta ili njihovih organizacijskih intranet mreža.

E-mail se čuva na mrežnim serverima sve do trenutka dok ga korisnik ne primi. Korisnik, kada bude htio, može pročitati njegov sadržaj na ekranu svoje radne stanice. Dakle, za samo nekoliko minuta truda (plus nekoliko mikrosekundi za prenos poruke) poruka za jednog ili više korisnika može biti sastavljena, poslana i primljena.

E-mail softver predstavlja komponentu nekog integrisanog paketa (kao na primjer MS Outlook) ili web browsera. Originalne verzije ovog softvera imaju mogućnost upućivanja poruke za više korisnika istovremeno (na osnovu predefined mailing lists), zatim obezbjeđuju sigurnosne zaštite u vidu passworda, automatsko forwardovanje poruka i drugo. Oni takođe omogućavaju čuvanje poruka u folderima, dodavanje atačmenta fajlu poruke, editovanje i slanje multimedijalnih poruka. Na kraju, e-mail softver automatski filtrira i sortira pristigle poruke, raspoređujući ih u odgovarajuće mailboxove i foldere.

Sistemski softver sastoji se od programa koji upravljaju i podržavaju kompjuterski sistem i njegovo procesiranje informacija. Slika 2 prikazuje da se sistemski softver može grupisati u dvije kategorije, koje obuhvataju programe za podršku sistema i programe za razvoj sistema.

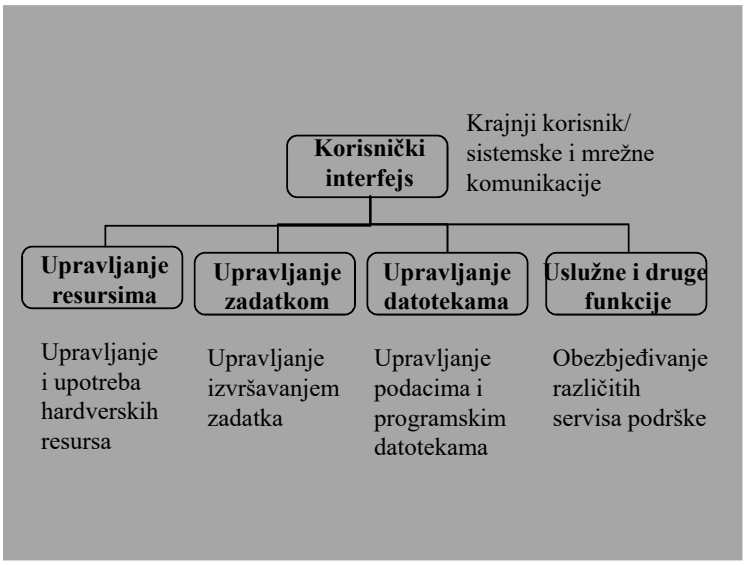
Programi za podršku sistema upravljaju hardverom, softverom, mrežom i resursima podataka prilikom izvršavanja korisničkih zadataka. Najvažniji programi iz ove kategorije jesu operativni sistemi, programi za upravljanje mrežom, programi za upravljanje bazama podataka i uslužni sistemski programi.

Najvažniji sistemski softverski paket za računar jeste **operativni sistem**. Operativni sistem predstavlja integrisani sistem programa koji upravljaju operacijama CPU, kontrolišu ulaz/izlaz i memorijske resurse, kao i aktivnosti računarskog sistema i obezbjeđuju veliki broj servisa podrške za izvršavanje korisničkih aplikativnih programa.

Osnovni zadatak operativnog sistema jeste maksimiziranje produktivnosti kompjuterskog sistema uz upravljanje njime na najefikasniji mogući način. Ovi programi minimiziraju potrebu korisnikovih intervencija prilikom procesiranja. Oni omogućavaju aplikativnim programima da izvršavaju standardne operacije kao što su pristup mreži, unos podataka, čuvanje i pretraživanje fajlova i štampanje i prikazivanje izlaza. Operativni sistem se nalazi na sekundarnoj memoriji i mora se učitati u radnu memoriju i aktivirati prije nego počne izvršavanje korisničkih aplikacija.

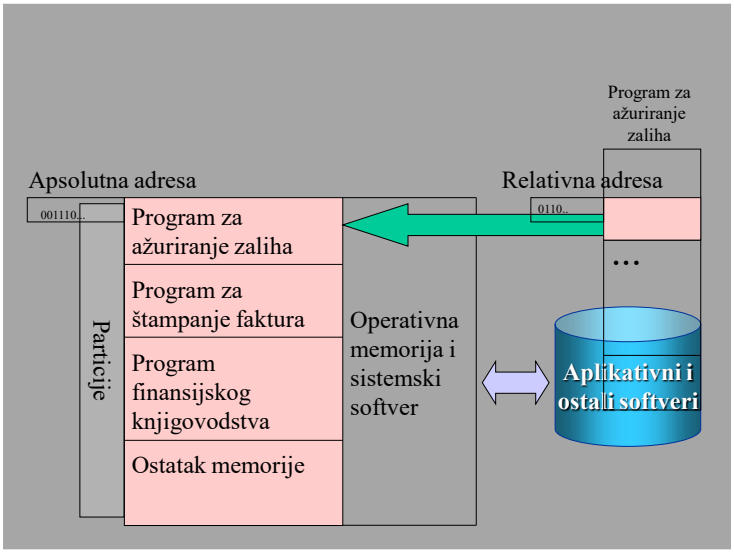
Operativni sistem obavlja pet osnovnih funkcija u računarskom sistemu, a to su: obezbjeđivanje korisničkog interfejsa, upravljanje resursima, upravljanje zadacima (procesima), upravljanje datotekama, obezbjeđivanje uslužnih servisa i servisa podrške (Slika 3) (O'Brien & Marakas, 2011).

Korisnički interfejs je dio operativnog sistema koji omogućava komunikaciju korisnika sa sistemom u smislu pokretanja programa, pristupa datotekama i izvršavanja raznih drugih zadataka. Tri osnovna tipa korisničkog interfejsa jesu komandni, interfejs preko sistema menija i grafički interfejs. Osnovni trendovi kod korisničkih interfejsa jesu izbjegavanje pamćenja i unošenja komandi ili čak i izbora opcija menija. Umjesto toga većina operativnih sistema obezbjeđuje grafički korisnički interfejs (GUI – Graphical User Interface), koji je jednostavan za upotrebu, a koristi ikone, barove, komandnu dugmad, boksove i drugo. GUI se zasnivaju na ulaznim uređajima (poput miša) koji omogućavaju selekciju objekata pokazivačem ili na dodir.



Slika 3. Funkcije operativnog sistema

Upravljanje resursima podrazumijeva upravljanje hardverskim i mrežnim resursima, uključujući CPU, radnu memoriju, sekundarnu memoriju, telekomunikacione procesore i input/output periferije. Na primjer, programi za upravljanje memorijom čuvaju trag o tome gdje su podaci i programi smješteni u memoriji (adrese). Oni dijele memoriju na particije i omogućavaju razmjenu djelova programa i podataka između memorije i magnetnih diskova ili nekih drugih uređaja sekundarne memorije. Drugim riječima, realizuju koncept virtuelne memorije koji omogućava sistemu da izvršava programe i obrađuje podatke veće nego što su realni kapaciteti osnovne (radne) memorije (Slika 4) (O'Brien & Marakas, 2011).



Slika 4. Realizacija koncepta virtuelne memorije

Upravljanje datotekama omogućava kreiranje, brisanje i pristup datotekama podataka i programa. Programi za upravljanje datotekama čuvaju fizičke lokacije (adrese) datoteka na magnetnim diskovima ili nekim drugim uređajima spoljašnje memorije. Operativni sistem, dakle,

održava direktorijume informacija o lokacijama i karakteristikama datoteka sačuvanih na uređajima sekundarne memorije.

Upravljanje zadacima (procesima) podrazumijeva upravljanje izvršavanjem zadataka (procesa) korisničkih aplikacija na centralnom procesoru. Operativni sistemi svakom procesu dodjeljuju mali trenutak (slot) CPU vremena i prekidaju CPU operacije da bi ga dodijelili drugom zadatku. Na ovaj način više zadataka se izvršava istovremeno, i to se označava terminom multitasking. Ukoliko CPU izvršava zadatke više programa istovremeno, onda je to multiprogramiranje, a ukoliko se istovremeno izvršavaju programi od strane više korisnika, riječ je o timesharing-u. Efikasnost multitasking-a zavisi od snage procesiranja CPU, virtuelne memorije i mogućnosti operativnog sistema.

Većina operativnih sistema ima mogućnosti **multitasking-a**. Tako korisnik može istovremeno obavljati dvije ili više operacija jednim programom (na primjer kucati tekst nekog dokumenta dok se neki drugi štampa) ili raditi sa više aplikacija, odnosno programa (na primjer kucati tekst i pretraživati web). Multitasking na mikrokompjuterima omogućen je razvojem moćnijih mikroprocesora sa sposobnošću adresiranja memorije većeg kapaciteta. Ovo omogućava operativnom sistemu da podijeli radnu memoriju na particije u kojima se mogu učitavati i izvršavati djelovi različitih aplikativnih programa. Broj programa koji se mogu konkurentno izvršavati zavisi od kapaciteta radne memorije, kao i od broja zahtjeva za procesiranje. Ukoliko je CPU preopterećen, tj. ima prevelik broj zahtjeva, može doći do sporog odziva, odnosno dugog čekanja. Ako je kapacitet memorije i snaga CPU adekvatna, koncept multitasking-a omogućava korisniku da nesmetano prelazi sa jedne aplikacije na drugu, da koristi datoteke u više aplikacija istovremeno i da izvršava zadatke u pozadini, kao što su dugotrajno štampanje, matematička izračunavanja ili komunikacione sesije.

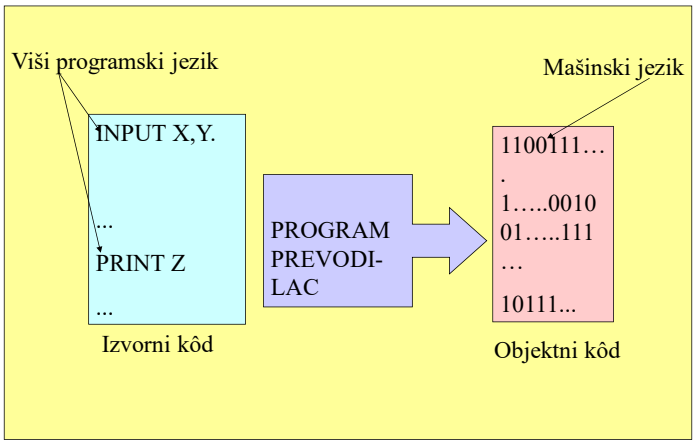
Prvi operativni sistem mikroračunara bio je MS-DOS (Microsoft Disk Operating System). To je bio jednokorisnički i single-tasking sistem sa komandnim korisničkim interfejsom. U kombinaciji sa Microsoft Windows-om imao je GUI i limitirane multitasking mogućnosti. Microsoft je 1995. godine zamijenio ovu DOS/Windows verziju operativnim sistemom Windows 95. Ovaj sistem je imao GUI, stvarni multitasking, mogućnost upravljanja mrežom, multimedijalne i druge opcije. Kasnije verzije ovog operativnog sistema jesu Windows 98, Windows 2000 i Windows XP.

Svoju ediciju **mrežnih operativnih sistema** Microsoft je započeo 1995. godine sa Windows-om NT (New Technology). Ovo je bio moćni multitasking, **višekorisnički sistem** koji je instaliran na mnogim mrežnim serverima da upravlja klijent/server mrežama, ali i na PC računarima sa zahtjevima visokih performansi. Microsoft je svoje proizvode 98 i NT spojio u novom proizvodu Windows 2000 koji predstavlja moćan operativni sistem za mrežne i web-servere, ali i za PC i laptop računare. Sve kasnije verzije Windows-a (XP, Vista, Windows 7, Windows 11) imaju jednokorisničku – PC i višekorisničku – profesionalnu verziju.

Kod većih kompjuterskih sistema koriste se mrežni operativni sistemi UNIX i Linux. I pored dosta visoke cijene, UNIX je najčešći izbor za web-servere. Linux je jeftinija verzija UNIX operativnog sistema koja se i danas može nabaviti besplatno ili po veoma niskoj cijeni preko interneta.

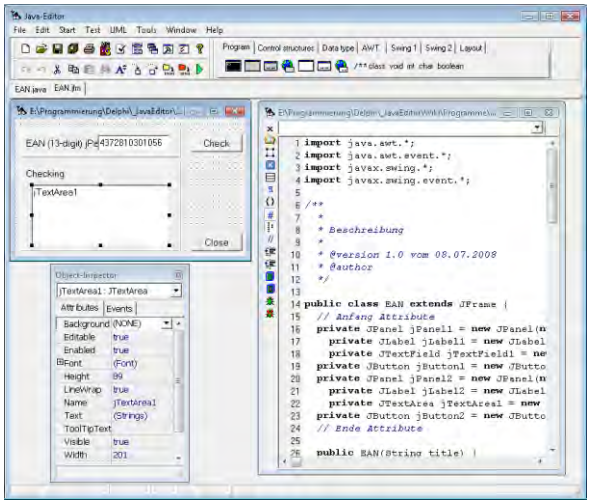
U sistemski softver spadaju i **programski alati koji pomažu programerima da razvijaju kompjuterske programe**, kao što su prevodioci programskih jezika i programski editori.

Kompjuterski program se sastoji od niza instrukcija napisanih programskim jezikom (izvorni kôd), koje moraju biti prevedene pomoću programa prevodioca u mašinski jezik (izvršni ili objektni kôd), kako bi mogle biti procesirane, tj. izvršene od strane CPU (Slika 5) (Kašćelan, 2016). Programi prevodioci su kompajleri i interpreteri. Kompajleri prevode naredbe viših programskih jezika u mašinski kôd. Interpreter je specijalni tip kompajlera koji prevodi i izvršava jednu po jednu instrukciju programa, za razliku od kompajlera, koji prvo produkuje cjelokupan mašinski kôd, pa ga tek onda izvršava u cjelosti. Java je primjer jezika koji se prevodi interpreterom. Programske instrukcije u okviru Java apleta interpretiraju se i izvršavaju „u letu“ kada počne izvršavanje apleta na klijentskom PC računaru.



Slika 5. Prevođenje izvornog kôda u objektni

Programski editori omogućavaju editovanje i debagovanje (identifikovanje grešaka) izvornog programskog kôda. Oni obično imaju GUI (omogućavaju vizuelno programiranje) i pomažu programerima da efikasno i jednostavno identifikuju, minimiziraju i isprave greške prilikom programiranja. Slika 6 prikazuje editor za programski jezik Java.



Slika 6. Java editor

Računarske mreže

Računarske mreže omogućavaju razmjenu multimedijalnih informacija posredstvom međusobno povezanih računara.

Računarske mreže, u koje spadaju globalna svjetska mreža **internet**, mreža unutar jedne organizacije – **intranet** i mreža organizacije sa poslovnim partnerima – **ekstranet**, predstavljaju osnovu za elektronsko komuniciranje i saradnju radnih timova, organizacija i poslovnih partnera, za efikasno upravljanje poslovanjem, dijeljenje poslovnih resursa i za konkurentno učešće na globalnom svjetskom tržištu.

Mreže se dijele prema veličini područja koje pokrivaju i namjeni koju imaju. Osnovni tipovi mreža su lokalne mreže, mreže širokog opsega, sigurne privatne mreže, klijent/server mreže, cloud mreže i peer-to-peer mreže.

Lokalna mreža (LAN – Local Area Network) povezuje računare i druge uređaje u ograničenom prostoru, kao što su kancelarija, škola ili jedna zgrada. Lokalne mreže omogućavaju dijeljenje datoteka, štampača i pristupa internetu. Računari u LAN mreži mogu se povezivati kablovima putem Ethernet tehnologije ili bežično preko Wi-Fi signala. Ethernet je standardna tehnologija za povezivanje računara u lokalnim mrežama. Podaci se prenose digitalnim električnim impulsima kroz bakarne kablove sa upredenim paricama ili svjetlosnim signalima kroz optička vlakna. Naziv potiče od 'etara' – starog koncepta nevidljivog medija za prenos signala. U originalnom Ethernetu poruke su se slale svim računarima (broadcast), ali moderni Ethernet koristi svičeve koji ih usmjeravaju samo do odredišta, čineći mrežu bržom i efikasnijom. Ethernet omogućava brzine od 100 Mbps do 10 Gbps i standard je za gotovo sve žičane lokalne mreže. Svaki računar u lokalnoj mreži ima specijalnu mrežnu karticu koja omogućava komunikaciju. U lokalnoj mreži obično postoji jedan moćniji računar koji radi kao server. Server upravlja zajedničkim resursima i omogućava svim računarima pristup dijeljenim datotekama, štampačima i internet vezi (Rainer & Turban, 2009).

Mreža širokog opsega (WAN – Wide Area Network) pokriva velike geografske površine, kao što su gradovi, zemlje ili čak cijeli kontinenti. WAN mreže povezuju više lokalnih mreža na velikim udaljenostima. Na primjer, velike organizacije koriste WAN mreže za komunikaciju između svojih odsjeka u različitim gradovima ili zemljama. Internet je najveća WAN mreža na svijetu jer povezuje mreže širom planete (Rainer & Turban, 2009).

Sigurna privatna mreža (VPN – Virtual Private Network) stvara zaštićene „tunelske" veze preko javnog interneta. VPN mreže omogućavaju zaposlenima da rade od kuće ili na putu kao da su fizički prisutni u kancelariji. Takođe omogućavaju organizacijama da sigurno komuniciraju sa poslovnim partnerima. VPN šifrira sve podatke koji prolaze kroz internet vezu i štiti ih od neovlašćenog pristupa.

Klijent/server mreže su najrašireniji tip mreža u poslovnim okruženjima. U ovim mrežama klijenti (računari korisnika) šalju zahtjeve serveru, a server obrađuje podatke i vraća rezultate. Postoje različite arhitekture klijent/server mreža:

- U **dvoslojnoj arhitekturi** klijent (računar korisnika) ima instaliranu kompletnu aplikaciju, dok server samo čuva bazu podataka i šalje sirove podatke. Ovaj pristup zahtijeva moćne računare na strani klijenata i komplikovana ažuriranja softvera na svakom računaru.

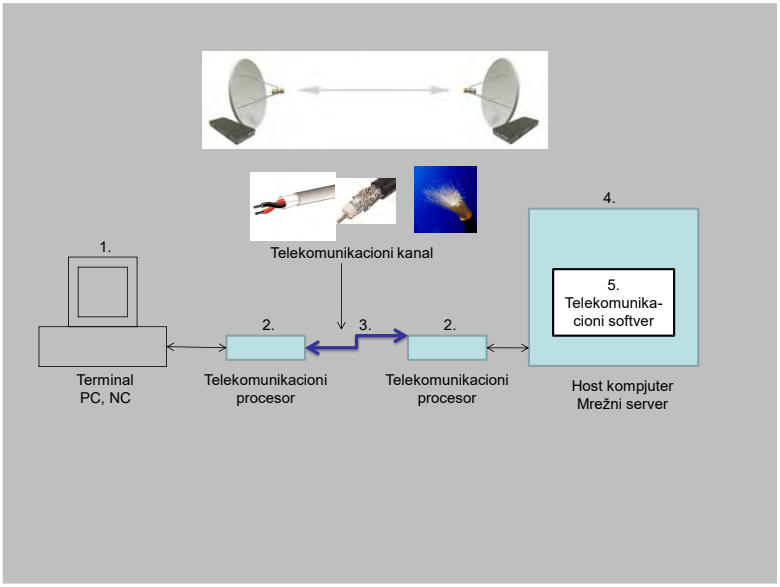
- **Troslojna arhitektura** dijeli posao na tri dijela. Klijent ima samo korisnički interfejs, aplikativni server obrađuje logiku i poslovna pravila, a poseban server baze podataka čuva informacije. Ovaj model omogućava jeftinije klijente i centralizovanu obradu podataka.
- **Web-bazirana arhitektura** je moderni standard. Klijent je web-pregledač ili mobilna aplikacija koja ne zahtijeva instalaciju softvera. Web-server pokreće logiku aplikacije, a baza podataka čuva informacije.
- **Cloud bazirane mreže** predstavljaju napredak web-baziranih arhitektura. Serveri se nalaze u velikim data centrima koje vode kompanije poput Googlea, Microsofta ili Amazona. Korisnici pristupaju aplikacijama i podacima preko interneta sa bilo kog uređaja. Primjeri cloud usluga su Google Workspace, Microsoft Azure i Amazon Web Services.

Peer-to-peer (P2P) mreže omogućavaju računarima da direktno komuniciraju jedni s drugima bez centralnog servera. Svaki računar u P2P mreži može biti i klijent i server. Ove mreže se koriste za dijeljenje datoteka (kao BitTorrent) ili u blockchain tehnologijama (kao Bitcoin). P2P model je decentralizovan i otporan na kvarove pojedinačnih računara (Kašćelan, 2016).

Moderne arhitekture poput web-baziranih i cloud mreža omogućavaju lako skaliranje, mobilnost i automatska ažuriranja. Evolucija od dvoslojnih do web-baziranih modela omogućila je prelazak sa teških desktop aplikacija na jednostavna browser rješenja dostupna sa bilo kog uređaja.

Uopšteno rečeno, računarska mreža je sistem u kome računar pošiljalac šalje poruku računaru primaocu preko kanala sastavljenog od različitih tipova medija (bakarnih, optičkih ili bežičnih). Na Slici 7 prikazan je pojednostavljen **konceptualni model komunikacione mreže**, koji se sastoji od pet osnovnih komponenti (O'Brien & Marakas, 2011):

- **Terminali** su krajnji uređaji preko kojih korisnici pristupaju mreži. Danas to nijesu samo personalni računari, već i pametni telefoni, tableti, pametni televizori, IoT uređaji i drugi digitalni sistemi koji mogu slati i primati podatke.
- **Komunikacioni uređaji** (kao što su switch-evi, ruteri, pristupne tačke, modemi i gateway uređaji) omogućavaju usmjeravanje, prevođenje i kontrolu toka podataka kroz mrežu. Oni mogu pretvarati signal iz digitalnog u analogni i obrnuto, vršiti filtriranje saobraćaja, kontrolu propusnog opsega, sigurnosnu provjeru paketa i optimizaciju saobraćaja.
- **Komunikacioni kanali** predstavljaju fizičke ili bežične puteve kojima se podaci prenose. Danas se koriste bakarni kablovi (upredena parica), koaksijalni i optički kablovi, ali i bežični prenos putem Wi-Fi mreža, mobilnih (4G/5G) mreža, mikrotalasa, radio-linkova i satelitskih sistema.
- **Računari i serverska infrastruktura** u mreži upravljaju obradom i skladištenjem podataka. U manjim mrežama ulogu servera može obavljati standardni mrežni računar, dok se u većim sistemima koriste data centri ili cloud platforme, koje pružaju visoke performanse i pouzdanost.
- **Mrežni softver i servisi** obuhvataju sve programe koji omogućavaju komunikaciju i upravljanje mrežom – od operativnih sistema na serverima, preko mrežnih protokola (TCP/IP, HTTP, DNS), do korisničkih aplikacija kao što su web-pregledači, e-mail klijenti ili cloud servisi. Ovaj softver upravlja autentifikacijom korisnika, sigurnošću, adresiranjem i dostupnošću mrežnih resursa.



Slika 7. Konceptualni model komunikacione mreže

U **komunikacione uređaje** spadaju modemi za pristup internetu, mrežni uređaji za povezivanje djelova mreže i sigurnosni uređaji za zaštitu podataka. Ovi uređaji omogućavaju računarima da komuniciraju međusobno i sa internetom.

Modemi konvertuju digitalne računarske signale u analogne frekvencije kako bi se oni mogli prenijeti putem telefonskih ili kablovskih linija (Slika 8). Drugi modem na strani primaoca vraća signale u digitalni oblik. Ovaj proces se zove modulacija i demodulacija, pa je modem dobio ime po njemu. Standardne telefonske mreže dizajnirane su za analogne glasovne signale, dok računari rade s digitalnim podacima, pa je konverzija potrebna. Međutim, moderne digitalne mreže (fiber optika, Ethernet) prenose samo digitalne signale bez konverzije.

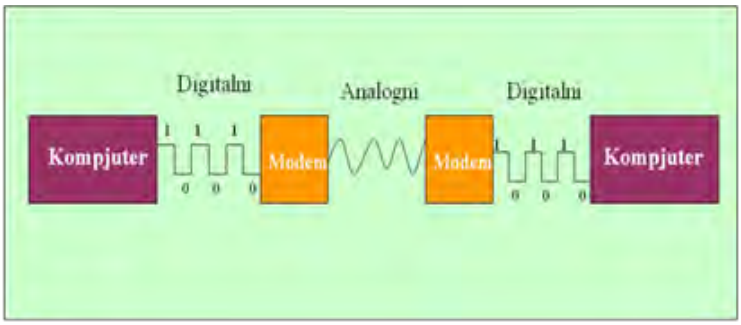
Modemi su potrebni za hibridne veze (DSL, kablovski internet) koje još uvijek koriste analogne signale na dijelu puta. U potpunim digitalnim mrežama poput fiber optike, modem nije potreban jer signali ostaju digitalni od izvora do odredišta.

Mrežni uređaji povezuju različite djelove mreže i usmjeravaju podatke:

- **Svič** (mrežni prekidač): Povezuje računare unutar iste lokalne mreže i inteligentno šalje poruke samo do odredišnog računara, štedeći propusni opseg mreže.
- **Ruter**: Povezuje različite mreže, na primjer lokalnu mrežu sa internetom, i određuje najoptimalniji put za poruke između mreža.
- **Gateway**: Omogućava komunikaciju između mreža koje koriste različite protokole ili arhitekture, prevodeći podatke iz jednog formata u drugi.

Sigurnosni uređaji štite mrežu od neovlašćenog pristupa i napada. Najvažniji takav uređaj je **Firewall** koji kontroliše promet između mreža i interneta, dopuštajući samo autorizovani saobraćaj. Blokira sumnjive pokušaje pristupa, štiti od hakerskih napada i može raditi kao hardverski uređaj ili softverska komponenta rutera. Moderni Firewall-i često uključuju zaštitu od DDoS napada i podršku za VPN tunelske veze. Mrežni uređaji osiguravaju efikasno usmjeravanje

podataka, dok Firewall štiti mrežu od vanjskih prijetnji, čineći kompletnu komunikacionu infrastrukturu.



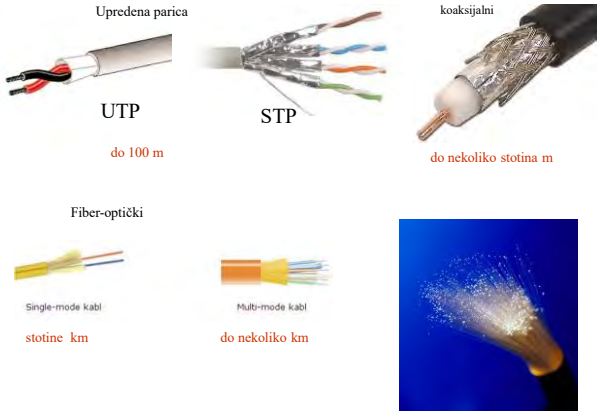
Slika 8. Uloga modema

Komunikacioni kanali koriste različite **komunikacione medije**, kao što su upredena parica, koaksijalni kabal, fiber-optički kabal i drugo, za fizičko povezivanje uređaja u mreži (Rainer & Turban, 2009).

Upredena parica (Twisted Pair) predstavlja najčešće korišćeni tip kabla u savremenim lokalnim (Ethernet) mrežama. Sastoji se od parova bakarnih žica koji su spiralno upredeni, čime se smanjuje uticaj spoljašnjih elektromagnetnih smetnji. Princip prenosa zasniva se na električnim signalima koji putuju kroz bakarne vodiče, dok upredanje parova sprečava miješanje signala (šum) između različitih vodova. Iako je prvobitno korišćena u telefonskim instalacijama, danas je standard u LAN mrežama zbog jednostavne instalacije i niske cijene.

Upredena parica je pogodna za prenos na kraćim udaljenostima (do oko 100 metara bez pojačanja signala), nakon čega dolazi do slabljenja, pa se koriste mrežni uređaji poput svičeva ili repetitora. Postoje dvije osnovne varijante ovog kabla (Slika 9):

- UTP (Unshielded Twisted Pair) – bez dodatnog oklopa, najčešće se koristi u kućnim i kancelarijskim mrežama;
- STP (Shielded Twisted Pair) – ima dodatno elektromagnetno oklapanje i koristi se u profesionalnim instalacijama gdje je potrebna veća zaštita od smetnji.



Slika 9. Vrste komunikacionih medija

Koaksijalni kabal je debela bakarna žica obmotana izolatorom, koja prenosi podatke u vidu elektromagnetnih talasa (Slika 9). Izolator minimizira miješanje i deformisanje signala prolaskom kroz žicu. Sa rastojanjem signal slabi, tako da se moraju koristiti pojačivači signala na svakih 500 m. Namijenjeni su za manja rastojanja. Mogu prenositi podatke u analognom i digitalnom formatu. Više koaksijalnih kablova može biti objedinjeno u jedan radi lakše instalacije. Teški su, nesavitljivi i kompleksni za ugradnju.

Optički (fiber-optički) kabal predstavlja jednu od ključnih tehnologija savremenih mreža. Omogućio je povezivanje mrežnih sistema na veoma velikim geografskim udaljenostima uz minimalna kašnjenja. Sastoji se od jednog ili više staklenih ili plastičnih vlakana (fibera) smještenih u zaštitnom omotaču. Prenos podataka odvija se u vidu svjetlosnih impulsa, koje u modernim sistemima najčešće generišu laserske diode (VCSEL ili DFB), dok se LED koristi uglavnom za kraće i manje zahtjevne veze.

Optički kabal ima znatno manju masu i debljinu u odnosu na bakarne kablove, a omogućava izuzetno velike brzine prenosa podataka. Otporan je na elektromagnetne smetnje i sam ih ne emituje, što doprinosi stabilnosti i pouzdanosti veze. Zbog manjeg slabljenja signala, potreba za pojačivačima je znatno smanjena, a prenos je manje podložan greškama. Takođe, ovi kablovi su otporniji na fizička oštećenja u odnosu na tradicionalne medije.

Zahvaljujući ovim prednostima, optika je danas postala standardni komunikacioni medij za internet okosnice, telekomunikacione sisteme i moderne LAN/WAN mreže. Jedina značajnija mana je viša cijena instalacije, zbog čega se u praksi često koristi kao glavni vod mreže, dok se do krajnjih uređaja i dalje provodi bakarna infrastruktura.

Bežične komunikacione tehnologije zasnovane na radio-talasima i mikrotalasima omogućavaju digitalne komunikacije između komunikacionih uređaja bez njihovog povezivanja žicom. Bežične tehnologije obuhvataju zemaljske mikrotalasne sisteme, satelitske komunikacione sisteme, celularne telefonske sisteme i bežične LAN-ove.

Zemaljski mikrotalasni sistemi prenose veoma brze radio-signale između relejskih stanica udaljenih međusobno aproksimativno 50 km. Mikrotalasne antene su obično smještene na krovovima visokih zgrada, tornjevima, brdima ili planinskim vrhovima. Još uvijek su popularan medijum kako u mrežama dalekog dometa, tako i u gradskim metropola mrežama.

Satelitski komunikacioni sistemi koriste mikrotalasne frekvencije za prenos podataka na velikim udaljenostima. Većina komunikacionih satelita nalazi se na geostacionarnoj orbiti, na visini od oko 35.786 km iznad ekvatora, gdje se kreću istom ugaonom brzinom kao Zemlja, što im omogućava da stalno „stoje“ iznad iste tačke. Sateliti se napajaju solarnom energijom i mogu prenositi podatke brzinama koje danas dostižu i više gigabita u sekundi.

Zemaljske stanice koriste specijalizovane satelitske antene da usmjere signal prema satelitu, koji ga zatim pojačava i prosljeđuje drugim udaljenim stanicama. Dok su se raniji satelitski sistemi koristili prvenstveno za TV i glasovnu komunikaciju, savremeni sistemi podržavaju širokopojasni prenos multimedijalnih sadržaja, internetskih servisa i velikih količina podataka u različitim formatima.

Zbog velike udaljenosti signala koje putuju putem geostacionarnih satelita, javlja se kašnjenje (latencija) od oko 500–600 ms, što ih čini manje pogodnim za aplikacije u realnom vremenu poput

online igara ili interaktivnih video-poziva. Zbog toga se danas sve više koriste sateliti u niskoj orbiti (LEO – Low Earth Orbit), postavljeni na visini od oko 500–1200 km, koji nude manje kašnjenje i brži odziv, pa ih koriste moderne satelitske mreže poput onih za globalni internet pristup.

U poslovnom okruženju satelitske veze se koriste za povezivanje udaljenih poslovnica, skladišta, terenskih timova i lokacija do kojih ne dopire klasična mrežna infrastruktura, obezbjeđujući stabilnu komunikaciju čak i u geografskim područjima bez kopnenih mrežnih veza.

Mobilni telefonski sistemi (celularni sistemi) koriste radio-komunikacione tehnologije za bežične digitalne komunikacije. Ovi sistemi dijele geografski prostor na ćelije različite veličine – od velikih ćelija koje pokrivaju sela i predgrađa, do malih ćelija u gradskim ulicama i zgradama. Svaka ćelija ima baznu stanicu sa antenama koja šalje i prima signale prema mobilnim uređajima (telefonima, tabletima, laptopovima). Kada se korisnici kreću iz jedne ćelije u drugu, njihova veza (poziv ili internet) se automatski prebacuje na novu baznu stanicu bez prekida, uz pomoć centralnih računarskih sistema. Svi moderni mobilni sistemi koriste digitalne tehnologije (4G LTE i 5G) koje rade preko internet protokola. Ovo omogućava veći kapacitet mreže, bolju sigurnost i podršku za napredne servise poput brzog interneta, video-poziva, streaminga i povezivanja pametnih uređaja (IoT). U kontekstu računarskih mreža, mobilni sistemi funkcionišu kao bežični pristup internetu za sve uređaje, koristeći iste IP adrese i protokole kao Wi-Fi i žični internet, čineći ih integralnim dijelom korporativnih i javnih mreža.

Sprovođenje kablova u kancelarijama i zgradama za lokalne mreže često je veoma težak i skup posao. Stare zgrade najčešće nemaju kanale za kablove, a kod novih neadekvatno postavljeni kanali mogu izazvati nužnost potpune relokacije računarskih stanica i mrežne opreme. Jedno od rješenja ovakvih problema jeste **bežični LAN (Wi-Fi)**, koji omogućava povezivanje bez postavljanja kablova. Koriste se digitalne radio-tehnologije na 2.4 GHz i 5 GHz frekvencijama. Wi-Fi LAN-ovi omogućavaju brzu instalaciju i često su jeftiniji za ugradnju od tradicionalnih žičnih mreža. Računari i laptopovi se povezuju na internet i druge mreže preko Wi-Fi adaptera i rutera.

Prenos podataka putem komunikacionih kanala može biti **analogni** i **digitalni**, i o tome je već bilo riječi. Digitalni prenos može biti **asinhroni** i **sinhroni**. Kod asinhronog prenosa podaci se prenose karakter po karakter, dok se kod sinhronog prenose blokovi karaktera. Dalje, prenos može biti **jednostruki**, pri kome se podaci prenose samo u jednom smjeru**, poludvostruki** – podaci se prenose u oba smjera, ali u različitim vremenima i **dvostruki**, kod koga podaci kroz prenosni medij prolaze u oba smjera u isto vrijeme. **Brzina prenosa podataka** se mjeri bitovima po sekundi (bps). **Kapacitet komunikacionih kanala (bandwidth)** predstavlja raspon frekvencija koje kanal može prenijeti, a od njega zavisi maksimalna brzina prenosa. Kanali se dijele na uskopojasne (niski kapacitet) i širokopojasne (visoki kapacitet).

Osim osnovne jedinice bps, koriste se i veće jedinice, kao što su:

- kbps (kilobita po sekundi) = hiljadu bita po sekundi
- Mbps (megabita po sekundi) = milion bita po sekundi
- Gbps (gigabita po sekundi) = milijardu bita po sekundi.

Softver predstavlja vitalnu komponentu računarskih mreža. Nalazi se na serverima, računarskim stanicama i komunikacionim uređajima kao što su ruteri i mrežni koncentratori (habovi i svičevi). U **komunikacioni softver** spadaju **mrežni operativni sistemi** i programi za nadzor mreže. Oni određuju prioritete u prenosu, usmjeravaju i preusmjeravaju poruke, biraju odgovarajuće uređaje i redove čekanja pri zahtjevu za prenos, otkrivaju i ispravljaju greške pri prenosu, bilježe statistiku o mrežnim aktivnostima i štite mrežu od neovlašćenih pristupa.

Osnovne funkcije upravljanja mrežom su (Kašćelan, 2016):

- Upravljanje saobraćajem – Softver upravlja mrežnim resursima i saobraćajem u mreži kako bi se izbjegla gužva i istovremeno optimizovao nivo usluga za korisnike.
- Sigurnost – Softver osigurava provjeru identiteta korisnika, šifriranje podataka i druge sigurnosne mjere.
- Nadzor mreže – Softver prati cjelokupnu mrežu i upozorava administratore o mogućim problemima prije nego što se oni pojave.
- Planiranje kapaciteta – Softver analizira mrežne resurse, obrasce saobraćaja i korisničke potrebe kako bi efikasnije zadovoljio te potrebe kada se one mijenjaju.

Bez standarda za povezivanje hardvera, softvera i komunikacionih linija, mreže bi bile skupe, neefikasne i uređaji različitih proizvođača ne bi mogli komunicirati međusobno. Proizvođači i međunarodne organizacije razvili su **protokole** (pravila komunikacije) i **mrežne arhitekture** (opšte planove) kako bi omogućili kompatibilnost i povezivanje između različitih mreža i uređaja (O'Brien & Marakas, 2011).

Protokoli su standardna pravila koja određuju kako računari i uređaji razmjenjuju podatke. Mrežne arhitekture organizuju protokole tako da računari i uređaji različitih proizvođača mogu jednostavno i kompatibilno komunicirati međusobno. Primjeri protokola su standardi za kablove i konektore, način slanja poruka i povezivanje različitih mreža.

Mrežne arhitekture čine komunikaciju otvorenom, jednostavnom i efikasnom korišćenjem standardnih pravila na različitim nivoima mreže. One određuju kako podaci putuju kroz mrežu. Korisnička aplikacija (npr. web-pretraživač) dijeli podatke u male pakete, dodjeljuje im adrese i šalje kroz mrežu. Na odredištu se paketi sabiraju i predaju aplikaciji primaoca. Svaki paket prolazi kroz više uređaja (rutere, svičeve) koji ga usmjeravaju prema cilju, provjeravaju greške i osiguravaju prenos.

Najpoznatiji standard je **TCP/IP**, koji pokreće internet. Razvijen je za američku vojnu mrežu, a danas ga koristi većina organizacionih mreža.

TCP osigurava da podaci stignu bez greške (ponovo šalje izgubljene pakete), dok **IP** daje svakom uređaju jedinstvenu adresu na internetu. TCP/IP je postao standardna mrežna arhitektura jer omogućava jednostavno povezivanje bilo kog računara na globalnu mrežu.

Danas gotovo sve mreže koriste TCP/IP protokole, što znači da računari, telefoni, tableti i serveri razgovaraju istim „jezikom" bez obzira na proizvođača.

Pristup internetu se u novije vrijeme najčešće ostvaruje pomoću širokopojasnih (broadband) veza koje omogućavaju visoke brzine prenosa podataka i istovremeni prenos videa, glasa i podataka.

Ove veze rade na principu packet switchinga – podaci se dijele u male pakete koji putuju različitim putevima kroz mrežu i na odredištu se ponovo spajaju u originalnu poruku.

Najbrži i najpouzdaniji način je **fiber optička veza (FTTH – Fiber To The Home)**. Optički kablovi prenose podatke svjetlosnim signalima i omogućavaju brzine od 1 Gbps (1000 Mbps) pa čak i do 10 Gbps u modernim instalacijama. Ovo je standard za nova naselja i poslovne zgrade.

Gdje fiber nije dostupan, koriste se **DSL** veze preko postojećih telefonskih linija. VDSL tehnologija omogućava brzine do 100 Mbps i omogućava istovremeno korišćenje telefona i interneta. ADSL je sporija varijanta sa brzinama do 24 Mbps za preuzimanje.

Kablovski internet koristi koaksijalne kablove (kao za kablovsku TV) i DOCSIS tehnologiju. Moderni kablovski sistemi dostižu brzine do 1 Gbps i više, a omogućavaju istovremeni prenos TV signala, telefona i interneta.

U ruralnim područjima ili gdje nema žičane infrastrukture, koriste se **bežične broadband veze** poput 5G Fixed Wireless Access (FWA). Specijalne 5G antene na kućama primaju signal od najbliže bazne stanice i omogućavaju brzine od 100 Mbps do 1 Gbps.

Svi ovi servisi koriste IP protokole (TCP/IP) kao standard za komunikaciju. Svaki uređaj u mreži dobija jedinstvenu IP adresu, a podaci se prenose u paketima koji sadrže adresu pošiljaoca i primaoca, kao i informacije za provjeru grešaka.

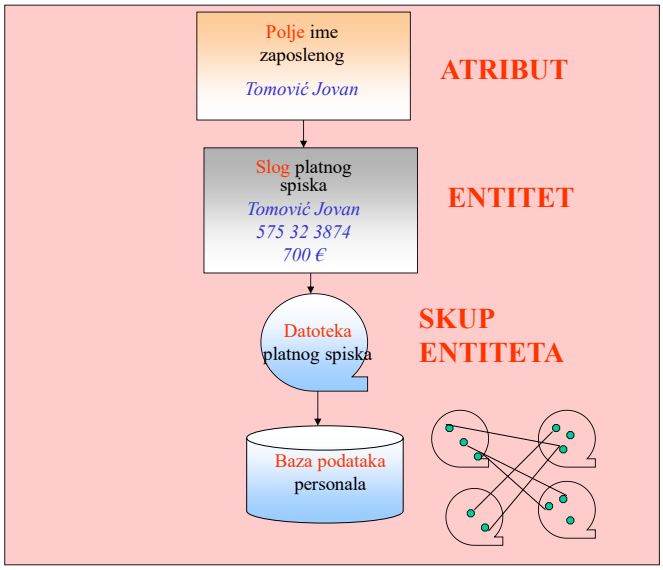
Broadband servisi omogućavaju da više korisnika istovremeno koriste mrežu bez prekida – streaming videa, video-pozive, rad od kuće i povezivanje pametnih uređaja, koji rade paralelno zahvaljujući visokom kapacitetu i efikasnom upravljanju saobraćajem.

Danas su gotovo sve internet veze digitalne i rade preko IP mreža, eliminišući potrebu za analogno-digitalnom konverzijom koja je bila potrebna kod starijih tehnologija.

Baze podataka

Podaci mogu imati različite formate, uključujući tradicionalne **alfanumeričke podatke**, koji se sastoje od brojeva, slova i drugih specijalnih znakova, **tekstualne podatke** u vidu rečenica i pasusa, koji se koriste u pisanim komunikacijama, **image podatke**, kao što su grafički oblici i figure, audio-podatke, kao što su ljudski glas i ostali zvuci i druge.

Podaci su u IS-u logički organizovani u nekoliko hijerarhijskih nivoa u vidu karaktera, polja, slogova, fajlova i baza podataka (Slika 10) (Kašćelan, 2016).



Slika 10. Hijerarhijska organizacija podataka

Karakter je najelementarnija jedinica podatka koja se sastoji od jednog alfabetskog, numeričkog ili nekog drugog znaka (bit je još elementarnija jedinica podatka, ali se ona odnosi na fizičku, a ne na logičku organizaciju podataka). Sa korisničkog stanovišta (tj. sa logičkog stanovišta), karakter je najosnovniji dio podatka koji može biti razmatran i kojim se može upravljati.

Polje je sljedeći viši nivo organizovanja podatka. Polje se sastoji od niza karaktera. Na primjer, niz karaktera koji predstavlja ime neke ličnosti čini polje IME, a niz cifara i specijalnih znakova razdvajanja (kao što su tačka i zarez) koji predstavljaju iznos prodaje – čine polje IZNOS PRODAJE. Polje obično predstavlja neki atribut (osobinu ili svojstvo) nekog entiteta (objekta, osobe, mjesta ili događaja). Na primjer zarada zaposlenog je atribut entiteta 'zaposleni'.

Slog. – Logički povezana polja grupišu se u slogove (zapise ili *recorde*). Dakle, slog predstavlja skup atributa koji opisuju neki entitet. Primjer za to je slog platnog spiska koji može sadržati polja koja predstavljaju atribute ime, broj socijalnog osiguranja i iznos plate. Slog može biti fiksne dužine, ako sadrži fiksiran broj polja fiksirane dužine, ili varijabilne dužine, u slučaju da sadrži varijabilan broj polja promjenljive dužine.

Fajl ili **datoteka** predstavlja grupu međusobno sličnih slogova. U teoriji baza podataka ovakva grupa sličnih slogova još se naziva i **tabela** ili **skup entiteta**. Tako fajl, tj. tabela 'zaposleni' sadrži slogove svih zaposlenih u firmi. Fajlovi se najčešće klasifikuju zavisno od primjene, kao na primjer: fajl platnog spiska, fajl zaliha itd. Takođe se mogu klasifikovati zavisno od tipa podataka koje sadrže, kao što su dokument fajl, grafički fajl i dr.

Baza podataka je integrisana kolekcija logički povezanih fajlova. Baza podataka objedinjuje slogove raspoređene u različitim fajlovima u jedan zajednički logički prostor koji obezbjeđuje podatke za više različitih aplikacija. Baza podataka ne zavisi od aplikacija koje je koriste kao ni od tipa memorijskih uređaja koji se koriste za smještaj podataka. Dakle, baza podataka sadrži skupove entiteta (tabele) kao i odnose između entiteta. Na primjer, baza podataka personala može

sadržati datoteke, tj. skupove entiteta: Zaposleni, Izdržavana lica, Radno iskustvo, Platni spisak i druge.

Sa aspekta IS, **podatak** i **informacija** su različiti koncepti, iako se ti termini često koriste ravnopravno za jedan ili drugi koncept. **Podaci** su sirove činjenice ili posmatranja o nekom fizičkom fenomenu ili poslovnim transakcijama. **Informacije** su podaci konvertovani u oblik koji ima značenje za specifičnog korisnika.

Na primjer, nazivi robe, količine i novčani iznosi, sačuvani u okviru prodajne fakture, predstavljaju podatke o prodajnim transakcijama. Međutim, menadžer prodaje ne želi takve pojedinačne podatke o prodajnim transakcijama. Za njega informaciju predstavljaju organizovani i procesirani podaci u vidu pregleda ukupnog iznosa prodaje prema tipovima proizvoda ili prema prodajnim mjestima.

Podaci predstavljaju vitalni organizacioni resurs kojim se mora upravljati kao bilo kojim drugim poslovnim sredstvom. Upravljanje podacima podrazumijeva poznavanje IT tehnologija, kao što su **sistemi za upravljanje bazama podataka (Database Management System –DBMS)**, kao i metodologije logičkog organizovanja podataka (**modele podataka**) koji će zadovoljiti informacione zahtjeve preduzeća.

DBMS je softverski paket koji predstavlja interfejs između korisnika i baze podataka. On pomaže korisnicima da jednostavno i lako pristupaju podacima u bazi. Šire, osnovne primjene DBMS-a su razvoj, pretraživanje i održavanje baze podataka i razvoj korisničkih aplikativnih programa, kako bi se obezbijedile ažurne informacije potrebne korisnicima i njihovim organizacijama. Tabela 2 prikazuje osnovne funkcije i komponente DBMS-a koje ih podržavaju (Kašćelan, 2016).

Razvoj baze podataka. – DBMS paketi, kao što su Oracle ili MS SQL Server, omogućavaju krajnjim korisnicima jednostavan razvoj baze podataka koja im je potrebna. Velike organizacije sa klijent/server ili mainframe baziranim sistemom problem razvoja baze podataka povjeravaju projektantima i administratorima baze podataka (DBA – database administrators) i drugim stručnjacima iz ove oblasti. Na taj način se obezbjeđuje i poboljšava integritet i sigurnost podataka u organizacijskim bazama. Projektanti i administratori baze podataka koriste DDL (data definition language) koji se nalazi u okviru DBMS-a za specifikaciju i generisanje podataka, odnosa i strukture baze, kao i za njihovu modifikaciju, ukoliko je to potrebno. Te informacije, tj. specifikacije i definicije podataka čuvaju se u okviru *rječnika podataka* kojima upravlja DBA.

Tabela 2. Funkcije i komponente DBMS-a

Funkcija	DBMS komponenta
Definisanje baze podataka	Jezici i grafički alati za definisanje entiteta, veza, integritetskih ograničenja i prava pristupa
Neproceduralni pristup	Jezici i grafički alati za pristup podacima bez kompletnog kodiranja
Razvoj aplikacija	Grafički alati za razvoj menija, formi za unos podataka i izvještaja, 4GL jezici

Proceduralni jezički interfejs	Jezici koji kombinuju neproceduralni pristup podacima sa svim mogućnostima višeg programskog jezika
Procesiranje transakcija	Kontrolni mehanizmi koji sprečavaju konflikte prilikom konkurentnog dostupa i oporavljaju izgubljene podatke u slučaju kraha sistema
Podešavanje baze podataka	Alati za praćenje i poboljšanje performansi baze podataka

Rječnik podataka je alat za administraciju baze podataka. Riječ je o kompjuterskom katalogu (direktorijumu) koji sadrži podatke o podacima, tj. **metapodatke**. Rječnik podataka uključuje softversku komponentu koja upravlja bazom metapodataka, tj. podacima o strukturi i drugim karakteristikama baze. Na primjer, rječnik podataka može sadržati nazive i opise svih tipova slogova, kao i njihove međusobne veze, ograničenja pristupa krajnjih korisnika i aplikativnih programa i drugo. Administrator baze podataka može pretraživati rječnik podataka i provjeravati status metapodataka sa bilo kojeg aspekta. On takođe može po potrebi mijenjati definicije podataka.

Pretraživanje baze podataka. – Mogućnosti pretraživanja baze (postavljanja upita) su glavna prednost DBMS-a. Pretraživanje baze podataka korisnici obavljaju pomoću upitnih jezika ili generatora izvještaja, koje DBMS sadrži u sebi. Neposredne odgovore dobijaju ili u vidu ekranskih prikaza ili u vidu štampanih izvještaja. Upitni jezici ne zahtijevaju kompleksno programiranje, već se definiše kratki i jednostavni ad hoc zahtjev. Generator izvještaja omogućava jednostavno formatiranje informacija, tj. izvještaja i njihovo generisanje, odnosno štampu.

SQL (Structured Query Language) je upitni jezik koji koristi veliki broj DBMS-ova. Osnovni oblik SQL upita je:

SELECT... FROM... WHERE

Poslije SELECT klauzule navodi se lista polja koja korisnik želi da dobije. Poslije FROM klauzule navodi se lista fajlova, tj. tabela iz kojih se podaci pretražuju. U WHERE klauzuli se specifikuje uslov koji pretraživanje ograničava na one slogove koji ga zadovoljavaju. Mnogi DBMS paketi omogućavaju GUI, tj. *point and click* metod za definisanje upita, koji je lakši za upotrebu. Ovako grafički definisani upiti prevode se zatim u odgovarajuću SQL komandu. Neki paketi podržavaju upitne naredbe upotrebom prirodnog jezika, sličnog koverzacijskom engleskom jeziku.

Održavanje baze podataka podrazumijeva kontinuirane promjene podataka koje odražavaju nove poslovne transakcije ili neke druge poslovne događaje, kao i druge vrste promjena koje osiguravaju tačnost podataka u bazi. Ovaj proces održavanja baze podataka obavljaju programi za procesiranje transakcija i korisnički aplikativni programi.

Razvoj aplikacija za baze podataka DBMS omogućava na taj način što **krajnjim korisnicima, analitičarima sistema i programerima** obezbjeđuje interne 4GL jezike i ugrađene alate za razvoj softvera. Na primjer, pomoću DBMS alata mogu se razviti ekrani za unos podataka, izvještaji ili web-strane za neku poslovnu aplikaciju.

Posao aplikacionih programera je znatno olakšan jer se ne moraju razvijati detaljne procedure za upravljanje podacima. Umjesto toga oni jednostavno koriste naredbe DML (Data Manipulation Language) jezika, kao što je SQL na primjer, koje pozivaju DBMS da izvrši potrebne aktivnosti u vezi sa upravljanjem podacima (unos novih podataka, brisanje, izmjene, pretraživanje).

Kontinuirani razvoj informacionih tehnologija i njihovih poslovnih primjena rezultirao je evolucijom različitih **tipova baza podataka**.

Operacione (transakcione, produkcione) baze podataka memorišu detaljne i aktuelne podatke potrebne za podršku poslovnih procesa i operacija u e-biznis preduzeću. Primjeri za to su baza kupaca, baza ljudskih resursa – personala, baza zaliha i mnoge druge baze generisane poslovnim operacijama.

Analitičke baze podataka sadrže podatke posebno pripremljene za analizu i najčešće se organizuju u vidu **Data Warehouse-a (DW)**, centralnog skladišta podataka unutar organizacije. Za razliku od operacionih baza koje služe za svakodnevno poslovanje, poput evidentiranja transakcija, narudžbi ili podataka o klijentima, DW se koristi za analitičke potrebe i donošenje odluka. U Data Warehouse se memorišu podaci koji su prethodno ekstrahovani iz različitih izvora, kao što su operacione baze (npr. ERP, CRM sistemi), eksterni izvori (statistički podaci tržišta) ili druge interne baze i tabele u okviru organizacije. Ti podaci se prije skladištenja prečišćavaju i transformišu kako bi bili tačni, usklađeni i prilagođeni za analizu.

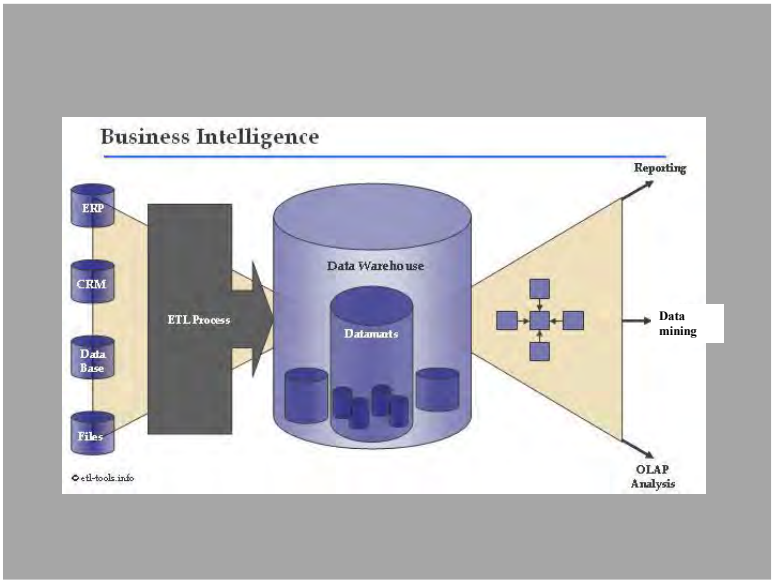
DW predstavlja centralni izvor ažurnih i istorijskih podataka koje koriste menadžeri i poslovni analitičari za napredne vrste analiza kao što su **OLAP (Online Analytical Processing)**, koji omogućava interaktivno posmatranje podataka iz različitih perspektiva (npr. po vremenu, proizvodu ili regionu), i **Data Mining (DM)**, koji omogućava otkrivanje skrivenih obrazaca i veza u velikoj količini podataka. Data Warehouse se po potrebi može podijeliti na manje cjeline koje se nazivaju data martovi, a oni sadrže samo dio podataka relevantan za određeni sektor ili poslovnu funkciju, kao što su prodaja, finansije ili marketing, čime se korisnicima omogućava brži pristup podacima koji su im najpotrebniji.

Proces pripreme podataka za DW poznat je kao **ETL (Extraction, Transformation, Loading)** i obuhvata tri faze. U fazi ekstrakcije podaci se preuzimaju iz različitih izvora. Zatim se u fazi transformacije podaci čiste, koriguju i prevode u zajednički format, uklanjaju se duplikati i nelogičnosti, a podaci se organizuju u strukture koje su pogodne za analitičku obradu. Na kraju, u fazi učitavanja, tako pripremljeni podaci se smještaju u DW, odakle se kasnije mogu prenositi i u odgovarajuće data martove ili druge analitičke baze. Ovaj proces se ne obavlja u realnom vremenu, već periodično, u vremenskim intervalima koji mogu biti svakih nekoliko sati, jednom dnevno, sedmično ili mjesečno, u zavisnosti od potreba organizacije.

Za rad sa DW koriste se specijalizovani analitički softverski alati koji omogućavaju postavljanje upita, izradu izvještaja, vizualizaciju podataka, primjenu Data Mining algoritama i OLAP analiza. Kombinacija ETL sistema za punjenje podataka u DW, samog DW-a i alata za OLAP i DM analize

čini kompletan **sistem poslovne inteligencije**, odnosno **Business Intelligence (BI)** sistem, koji pomaže organizacijama da pretvore podatke u upotrebljive informacije za donošenje odluka (Slika 11) (Kašćelan, 2016).

Data Mining proces omogućava automatsko otkrivanje novih obrazaca ponašanja, trendova i skrivenih veza u velikim količinama podataka (**Big Data**), nastalih tokom poslovnih aktivnosti. Analiza se vrši nad aktuelnim i nad istorijskim podacima, što omogućava uočavanje promjena kroz vrijeme i predviđanje budućih tendencija. U tu svrhu koriste se napredni algoritmi mašinskog učenja, kao što su drvo odlučivanja, neuronske mreže ili genetski algoritmi, koji prepoznaju obrasce i modele u podacima. Rezultati ovih analiza pružaju menadžerima podršku pri donošenju strateških odluka i planiranju budućih poslovnih aktivnosti radi boljeg pozicioniranja na tržištu. Data Mining, OLAP i druge tehnologije za analizu podataka iz Data Warehouse-a danas predstavljaju ključnu podršku savremenom poslovnom odlučivanju.



Slika 11. Sistem poslovne inteligencije

Distribuirane baze podataka. – Mnoge organizacije repliciraju i distribuiraju kopije ili djelove baze podataka na različite mrežne servere. Distribuirane baze mogu se, dakle, nalaziti na različitim serverima web, intranet, ekstranet ili neke druge kompanijske mreže. Distribuirane baze su najčešće kopije operacionih ili analitičkih baza podataka. Replikacija i distribucija baza podataka umanjuje performanse i sigurnost baze podataka. Garancija da će svi podaci u organizacijskim distribuiranim bazama podataka biti konzistentno i istovremeno ažurirani jeste jedan od glavnih zadataka distribuiranih DBMS-a.

Organizacija

Organizaciona komponenta informacionog sistema obuhvata **ljude** koji koriste, razvijaju i održavaju informacioni sistem, kao i **procedure** koje definišu pravila i način rada sa IS-om. Iako se u praksi često naglašava značaj hardvera i softvera, iskustvo pokazuje da su ljudi i jasno definisane procedure ključni za uspješno funkcionisanje kompletnog sistema. Čak i najmoderniji

tehnološki resursi ne mogu dati očekivane rezultate ukoliko korisnici nijesu adekvatno obučeni, ne prihvataju sistem ili ne poštuju utvrđene procedure korišćenja i zaštite podataka.

Pod ljudskim resursima u IS-u podrazumijevaju se dvije osnovne grupe aktera: **krajnji korisnici** i **IS specijalisti**. **Krajnji korisnici (korisnici ili klijenti)** su osobe koje u svakodnevnom radu koriste informacije koje IS generiše. Oni mogu biti računovođe, prodavci, inženjeri, menadžeri ili drugi zaposleni, a zajednička karakteristika im je da većinu radnog vremena provode u radu sa informacijama – njihovom obradom, razmjenom i distribucijom u okviru poslovnih procesa.

IS specijalisti su stručna lica koja razvijaju, održavaju i upravljaju informacionim sistemom. U ovu grupu spadaju sistem analitičari, programeri, administratori baza podataka, sistem operateri i drugi IT stručnjaci. Sistem analitičari definišu zahtjeve i dizajniraju rješenja na osnovu potreba korisnika, programeri razvijaju programska rješenja prema tim specifikacijama, dok sistem operateri i administratori obezbjeđuju nesmetan rad sistema i mrežne infrastrukture.

Međutim, za efikasan i bezbjedan rad informacionog sistema nije dovoljno imati samo kompetentne ljude. Neophodno je da njihov rad bude usmjeren i kontrolisan jasno definisanim procedurama. Posebno važnu ulogu imaju **procedure** koje obezbjeđuju **kontinuitet poslovanja** u slučaju prekida rada sistema (npr. kvar, napad, gubitak podataka) i procedure **informacione bezbjednosti** kojima se štite podaci od neovlašćenog pristupa, zloupotrebe ili kompromitovanja. Upravo ove procedure predstavljaju osnovu kontrolnog okvira koji je od suštinskog značaja za rad revizora informacionih sistema, jer omogućavaju procjenu da li organizacija može nastaviti poslovanje u vanrednim okolnostima i da li su informacijski resursi adekvatno zaštićeni.

Kontinuitet poslovanja

Upravljanje kontinuitetom poslovanja (Business Continuity Management – BCM) predstavlja skup planiranih i unaprijed definisanih aktivnosti kojima organizacija obezbjeđuje da može nastaviti rad čak i u slučaju ozbiljnih prekida, kao što su kvar informacionih sistema, prekid napajanja, požar, poplava, sajber napad ili drugi incident koji može ugroziti pružanje usluga. Cilj je da se spriječi duži zastoj u radu i omogući što brži povratak na funkcionalno stanje uz minimalne posljedice po korisnike i organizaciju.

U suštini, kontinuitet poslovanja odgovara na pitanje: „Šta će organizacija uraditi ako IT sistem prestane da funkcioniše?“. Za revizora informacionih sistema važno je da utvrdi ne samo da li planovi postoje, već i da li su realni, primjenljivi i poznati zaposlenima koji treba da ih sprovode.

Upravljanje kontinuitetom poslovanja obuhvata pripremu preventivnih mjera, jasno definisane postupke za reagovanje u trenutku prekida i planiran proces oporavka. Ove aktivnosti su povezane sa upravljanjem rizicima, informacionom bezbjednošću i upravljanjem IT operacijama, ali za razliku od njih, fokus upravljanja kontinuitetom poslovanja nije na sprečavanju incidenta, već na tome kako odgovoriti kada do prekida ipak dođe.

Da bi kontinuirani rad bio moguć, organizacija treba da uspostavi jasan okvir politika i odgovornosti, izvrši analizu uticaja na poslovanje (Business Impact Analysis), sprovede procjenu rizika, definiše strategiju kontinuiteta, izradi planove reagovanja i oporavka, obezbijedi obuku zaposlenih i redovno testira i ažurira uspostavljene mjere. Revizor provjerava prisutnost i kvalitet svakog od ovih elemenata, jer samo njihovim zajedničkim djelovanjem može postojati funkcionalan sistem kontinuiteta poslovanja, a ne samo formalno dokumentovan plan.

Prvi element uspostavljanja sistema kontinuiteta poslovanja jeste **politika kontinuiteta poslovanja** i jasno definisane odgovornosti. Organizacija treba formalno da usvoji dokument (politiku ili sličan akt) kojim potvrđuje da obezbjeđivanje kontinuiteta predstavlja strateški prioritet. Ovaj dokument mora biti odobren od strane rukovodstva, jer bez njihove podrške sistem kontinuiteta ostaje na nivou administrativnog dokumenta bez stvarnog uticaja na praksu.

Politika definiše osnovne principe, obim i ciljeve sistema kontinuiteta poslovanja, kao i ko je odgovoran za donošenje odluka u kriznim situacijama i ko koordinira oporavak. U mnogim institucijama se formira tim ili odbor za kontinuitet poslovanja, u kojem su prisutni predstavnici rukovodstva, IT službe, sektora za bezbjednost informacija i drugih ključnih organizacionih jedinica. Revizor treba da utvrdi da li takvo tijelo postoji, da li ima definisane nadležnosti i da li mu je obezbijeđena podrška u vidu resursa, pristupa informacijama i autoriteta da nalaže mjere.

U skladu sa politikom organizacija treba da definiše skup osnovnih preventivnih i zaštitnih mjera koje treba da smanje potencijalnu štetu u slučaju prekida. Politika je okvir koji revizor koristi da procijeni jesu li preventivne mjere, postupci i oporavak u skladu sa planiranim ciljevima. U skladu sa tim, revizor provjerava da li organizacija (WGITA-IDI, 2022):

- redovno izrađuje i čuva rezervne kopije podataka i aplikacija na fizički odvojenoj lokaciji,
- ima planiranu alternativnu lokaciju ili način rada u slučaju da glavni centar za obradu podataka postane nedostupan,
- održava plan oporavka informacionog sistema, uključujući procedure za vraćanje podataka i pokretanje aplikacija na drugoj opremi,
- primjenjuje fizičke kontrole poput sistema za gašenje požara, rezervnog napajanja električnom energijom, nadzora opreme i kontrolisanog pristupa server prostorijama,
- obučava zaposlene o ponašanju u vanrednim situacijama, uključujući prepoznavanje incidenata i prijavu nadležnom licu,
- kod outsourcinga, obezbjeđuje da eksterni pružaoci usluga imaju uspostavljene mehanizme kontinuiteta poslovanja i da su oni ugovorno obavezni da ih održavaju.

Rutinsko kreiranje rezervnih kopija i njihovo bezbjedno čuvanje često je najefikasnija i najisplativija mjera, jer se izgubljena oprema može zamijeniti, ali izgubljeni podaci u mnogim slučajevima ne mogu biti rekonstruisani. Zato revizor posebno obraća pažnju na to da li se kopije zaista kreiraju, gdje se nalaze, ko ih kontroliše i da li su ikada testirane za povrat podataka.

Pored toga, revizor treba da provjeri da li postoji plan održavanja i zamjene opreme, jer prekidi ne nastaju samo zbog velikih katastrofa, već često i zbog neplanskog kvara ili neovlašćene promjene djelova sistema. U praksi se često zanemaruje činjenica da neplanirano održavanje i promjene u IT okruženju mogu uzrokovati prekide jednako ozbiljne kao i vanjski incidenti.

Analiza uticaja na poslovanje (Business Impact Analysis – BIA) predstavlja proces kojim organizacija procjenjuje koje aktivnosti, procesi i informacioni sistemi imaju ključnu ulogu u njenom funkcionisanju i kakve bi posljedice nastale ako bi ti procesi bili prekinuti. Cilj ove analize je da se utvrdi koji djelovi poslovanja moraju biti obnovljeni prvo, u kojem vremenskom roku i uz koje resurse.

Kroz ovu analizu identifikuju se (WGITA-IDI, 2022):

- kritični procesi koji su neophodni za obavljanje osnovne djelatnosti,

- maksimalno prihvatljivo vrijeme prekida (Maximum Acceptable Outage) – koliko dugo proces može biti zaustavljen prije nego što nastupi ozbiljna šteta,
- poslovne posljedice prekida, koje mogu biti finansijske, operativne, reputacione ili zakonske,
- resursi potrebni za nastavak rada, uključujući IT sisteme, podatke, osoblje, alternativni prostor i komunikacione kanale.

Rezultat analize uticaja na poslovanje jeste lista prioriteta za oporavak, koja postaje osnova za izradu planova kontinuiteta i oporavka. U praksi, ova lista jasno pokazuje koje funkcije moraju biti aktivirane odmah (npr. sistem za isplatu sredstava, servis za prijem podataka, sistem elektronske komunikacije), a koje mogu ostati van funkcije duži period bez ozbiljnih posljedica.

Analiza uticaja se ne sprovodi jednokratno, već se ažurira kada dođe do promjena u organizacionoj strukturi, ulogama, procesima ili IT infrastrukturi. Na taj način se obezbjeđuje da prioriteti oporavka uvijek odgovaraju stvarnim poslovnim potrebama.

Procjena rizika predstavlja proces identifikovanja događaja koji mogu dovesti do prekida rada i procjene vjerovatnoće njihovog nastanka i mogućih posljedica. Rizici mogu poticati iz različitih izvora – od tehničkih kvarova i grešaka zaposlenih, do prirodnih nepogoda ili namjernih napada. Cilj procjene rizika je da organizacija na vrijeme prepozna prijetnje i definiše koje mjere zaštite i oporavka su potrebne.

U okviru procjene rizika identifikuju se (WGITA-IDI, 2022):

- potencijalni izvori prekida rada (npr. kvar servera, gubitak napajanja, požar, poplava, sajber napad, ljudska greška),
- vjerovatnoća nastanka svakog rizika,
- uticaj rizika na poslovanje, uzimajući u obzir kritične procese definisane u analizi uticaja na poslovanje,
- postojeće mjere zaštite i procjena da li su dovoljne ili je potrebno uvesti dodatne kontrole.

Procjena rizika omogućava organizaciji da realno sagleda na koje incidente treba biti posebno pripremljena i u koje oblasti treba ulagati više resursa. Ona se često dokumentuje u formi matrice rizika, u kojoj se jasno prikazuju prijetnje, postojeće kontrole i preostali rizik koji organizacija prihvata ili mora dodatno ublažiti. Kao i analiza uticaja, i procjena rizika se periodično preispituje i ažurira.

Nakon što su definisani kritični procesi i identifikovani rizici koji ih mogu ugroziti, organizacija razvija **strategiju kontinuiteta poslovanja**. Strategija predstavlja opšti pristup koji određuje na koji način će se obezbijediti nastavak rada u slučaju prekida i koje mjere će se primjenjivati u različitim scenarijima.

Uobičajene mjere strategije kontinuiteta uključuju (WGITA-IDI, 2022):

- rezervne (alternativne) lokacije za rad u slučaju da je osnovna lokacija nedostupna,
- redovne rezervne kopije podataka i aplikacija, sa čuvanjem kopija na izdvojenoj fizičkoj ili cloud lokaciji,
- sisteme za automatsko prebacivanje rada na rezervnu infrastrukturu (failover),

- alternativne komunikacione kanale i provajdere internet usluga, za slučaj prekida primarne veze,
- ugovorene aranžmane sa eksternim partnerima koji mogu privremeno obezbijediti infrastrukturu ili uslugu,
- privremene procedure rada, koje omogućavaju obavljanje kritičnih funkcija u ograničenim uslovima dok se ne uspostavi puno operativno stanje.

Strategija mora biti usklađena sa prioritetima utvrđenim analizom uticaja na poslovanje i prilagođena realnim mogućnostima organizacije. Ona ne treba da bude tehnički preopterećena, već jasno usmjerena na to kako obezbijediti nesmetan rad osnovnih funkcija uz minimalan prekid.

Nakon definisanja strategije, organizacija prelazi na izradu konkretnih **planova** koji detaljno opisuju kako treba postupati u trenutku prekida rada i tokom oporavka. Planovi moraju biti pisani jasno i razumljivo, tako da ih mogu primijeniti i zaposleni koji nijesu IT stručnjaci. Pored toga, plan treba da sadrži tačno definisane uloge, kontakt informacije, redosljed aktivnosti i kriterijume za procjenu kada je sistem ponovo operativan.

U praksi se izdvajaju tri osnovna plana (WGITA-IDI, 2022):

- **Plan kontinuiteta poslovanja (Business Continuity Plan – BCP)** – opisuje kako organizacija održava minimalni nivo funkcionisanja tokom prekida rada. Ovaj plan sadrži organizacione i proceduralne mjere za očuvanje osnovnih usluga dok traje incident.
- **Plan oporavka od katastrofe (Disaster Recovery Plan – DRP)** – fokusiran je na tehničku obnovu informacionih sistema, uključujući vraćanje podataka iz rezervnih kopija, pokretanje aplikacija na rezervnim serverima i obnovu mrežnih resursa. Dok BCP obezbjeđuje nastavak posla, DRP precizno definiše kako se IT infrastruktura vraća u funkcionalno stanje.
- **Plan rada u vanrednim uslovima (Emergency Operations Plan)** – opisuje privremene načine rada koji se koriste dok se ne uspostavi potpuno normalno stanje. To obuhvata rad sa ograničenim resursima, ručne procedure ili rad preko alternativnih sistema.

Tabela 3 prikazuje primjere situacija u kojima se svaki od ova tri plana aktivira.

Tabela 3. Tri tipa planova u okviru kontinuiteta poslovanja

Plan	**Svrha**	**Šta obuhvata**	**Kada se aktivira (primjer situacije)**
Plan kontinuiteta poslovanja (BCP)	Održavanje minimalnog nivoa ključnih funkcija organizacije tokom prekida rada	Organizacione mjere, alternativni načini pružanja usluga, privremene procedure rada	Sistem je nedostupan, ali se usluge moraju nastaviti pružati (npr. prelazak na ručno procesiranje zahtjeva dok IT sistem ne proradi)
Plan oporavka od katastrofe (DRP)	Tehnička obnova informacionih sistema i podataka	Aktiviranje rezervnih kopija, pokretanje servera na alternativnoj lokaciji,	Gubitak ili oštećenje IT infrastrukture (npr. havarija server sobe,

		vraćanje baza podataka	sajber napad, kvar diskova)
Plan rada u vanrednim uslovima (EOP)	Omogućavanje privremenog, ograničenog rada informacionog sistema dok se ne vrati puna funkcionalnost	Privremene konfiguracije, rad sa ograničenim funkcijama, korišćenje rezervne opreme ili cloud servisa	Sistem još nije potpuno obnovljen, ali je moguće pokrenuti djelimičan rad (npr. rad preko rezervnog servera sa smanjenim kapacitetom)

Planovi treba da budu dostupni u pisanoj i elektronskoj formi, čuvani na sigurnim lokacijama i poznati odgovornim licima. U njima treba navesti ko proglašava vanredno stanje, ko koordinira aktivnosti, ko odobrava prelazak na rezervnu lokaciju i ko potvrđuje povratak u normalno stanje rada.

Planovi kontinuiteta su korisni samo ako ih zaposleni razumiju i znaju kako da postupaju u slučaju prekida. Zbog toga je neophodno organizovati **obuke i simulacije** koje obuhvataju različite scenarije – od kratkotrajnog prekida rada sistema do potpune nemogućnosti korišćenja osnovne IT infrastrukture.

Obuka ne treba da bude formalna aktivnost ograničena na teoretska uputstva, već praktičan proces u kojem zaposleni uče tačne korake koje treba preduzeti (npr. kome prijaviti incident, kako pristupiti rezervnim sistemima, kako ručno obraditi podatke dok sistem ne proradi).

Pored obuke, važno je i podizanje svijesti, posebno kod korisnika koji nijesu direktno uključeni u IT procese, ali svojim postupcima mogu uticati na tok oporavka. Jasna komunikacija uloge svakog učesnika doprinosi smanjenju grešaka i zastoja tokom realizacije plana.

Testiranje planova predstavlja ključni element sistema kontinuiteta poslovanja. Kroz testiranje se provjerava da li planovi funkcionišu u praksi, da li su realni, da li su sve uloge razumljive i da li vrijeme oporavka odgovara potrebama organizacije. Test može biti osnovni (provjera kontakata, komunikacionih kanala) ili kompleksni (simulacija potpunog prekida rada i prelazak na rezervnu infrastrukturu).

Rezultati testiranja se dokumentuju i analiziraju kako bi se identifikovali nedostaci. Na osnovu toga planovi se prilagođavaju i unapređuju. Organizacija koja ne testira svoje planove ne može znati da li su oni zaista primjenljivi u realnoj situaciji.

U Tabeli 4 su sažeto prikazani elementi uspostavljanja sistema kontinuiteta poslovanja o kojima je bilo riječi.

Tabela 4. Faze i elementi sistema kontinuiteta poslovanja

Faza / Element	**Svrha**	**Tipične mjere / sadržaj**
Politika i odgovornosti	Uspostavljanje formalnog okvira i definisanje nadležnosti	Usvajanje politike, imenovanje tima, definisanje uloga i resursa

Analiza uticaja na poslovanje (BIA)	Identifikacija kritičnih procesa i definisanje prioriteta oporavka	Lista kritičnih sistema, maksimalno prihvatljivo vrijeme zastoja, procjena posljedica
Procjena rizika	Utvrđivanje prijetnji i vjerovatnoće prekida rada	Identifikacija scenarija prekida, matrica rizika, postojeće mjere zaštite
Definisanje strategije kontinuiteta	Odabir načina odgovora na prekide rada	Rezervne lokacije, rezervne kopije, alternativne komunikacije, ugovori sa partnerima
Izrada planova (BCP, DRP, EOP)	Operativno dokumentovanje koraka u slučaju prekida	Plan kontinuiteta, plan oporavka IT sistema, plan rada u vanrednim uslovima
Obuka i podizanje svijesti	Priprema osoblja za pravilno postupanje u kriznim situacijama	Obuke, simulacije, uputstva, komunikacioni protokoli
Testiranje i vježbe	Provjera da li planovi funkcionišu u praksi	Test rezervnih kopija, simulacije incidenta, analiza vremena oporavka
Održavanje i unapređivanje sistema	Stalno prilagođavanje planova promjenama u organizaciji	Redovno ažuriranje planova, revizije, evaluacije nakon testova

Sistem kontinuiteta poslovanja nije statičan dokument, već stalni proces. Planovi, kontakti, resursi i odgovornosti moraju se redovno ažurirati, posebno nakon promjena u organizaciji, IT infrastrukturi ili zakonskim obavezama. **Periodične provjere i interno praćenje** omogućavaju da sistem ostane funkcionalan i prilagođen stvarnim potrebama. Organizacija koja kontinuirano održava i unapređuje sistem kontinuiteta pokazuje visok nivo zrelosti u upravljanju rizicima i spremnosti na vanredne okolnosti.

Organizacija koja nema razvijen, dokumentovan i testiran sistem kontinuiteta poslovanja izložena je brojnim rizicima koji mogu značajno ugroziti njen rad, stabilnost i ugled. Kritične usluge i procesi, posebno u javnom sektoru, moraju biti dostupni i u vanrednim uslovima, jer prekid njihovog rada može izazvati ozbiljne finansijske, operativne i društvene posljedice.

Glavni **rizici** obuhvataju sljedeće (WGITA-IDI, 2022)

- Nedostatak ključnih dokumenata i procedura – Ako organizacija nema jasno definisane planove kontinuiteta poslovanja, oporavka od katastrofe ili rada u vanrednim uslovima, u trenutku prekida ne postoji jasan redosljed aktivnosti ni definisani koraci za reagovanje. To dovodi do improvizacije i gubitka vremena.
- Nejasne uloge i odgovornosti – Kada zaposleni ne znaju ko proglašava vanredno stanje, ko koordinira oporavak i ko donosi odluke, dolazi do zastoja, dupliranja aktivnosti ili

potpunog prekida komunikacije. Dobro napisan plan je neupotrebljiv ako uloge nijesu razumljive i prihvaćene u praksi.

- Neizvršena analiza i procjena ključnih procesa – Ako organizacija nije prethodno utvrdila koji sistemi i procesi imaju prioritet, u kriznoj situaciji se resursi mogu usmjeriti na sporedne funkcije, dok se kritične usluge zanemaruju. Time se povećava šteta i produžava vrijeme oporavka.
- Nepostojanje testiranja i obuke zaposlenih – Planovi koji postoje samo formalno, bez praktične primjene, mogu otkazati u trenutku kada su najpotrebniji. Bez obuke i simulacija, zaposleni nijesu spremni da reaguju pravilno i na vrijeme.
- Rizik za bezbjednost podataka i integritet sistema – Ako se oporavak sprovodi bez tačnih procedura i kontrola, može doći do gubitka podataka, neovlašćenog pristupa informacijama ili dodatnih tehničkih kvarova nastalih usljed nestručnih intervencija.
- Zavisnost od eksternih partnera (outsourcing) – Kada dio IT operacija obavlja vanjski dobavljač, organizacija može izgubiti kontrolu nad kontinuitetom i oporavkom ako ugovor ne sadrži jasne obaveze dobavljača u vezi sa rezervnim kopijama, alternativnim lokacijama i maksimalnim vremenom oporavka. U ekstremnim slučajevima, gubitak dobavljača može značiti potpunu nemogućnost nastavka rada.
- Gubitak institucionalnog znanja i sposobnosti reagovanja – Ako organizacija nema interne kapacitete za razumijevanje i upravljanje kontinuitetom poslovanja, već se oslanja isključivo na vanjske aktere, može doći do situacije u kojoj ljudi unutar organizacije ne znaju kako da reaguju ni kako da preuzmu kontrolu u slučaju prekida.

Organizacije koje ignorišu ove rizike ne samo da otežavaju vlastiti oporavak, već i dovode u pitanje pouzdanost javnih usluga, povjerenje korisnika i usklađenost sa zakonskim obavezama. Zato se kontinuitet poslovanja smatra jednom od ključnih kontrolnih tačaka koje revizori moraju uzeti u obzir prilikom procjene zrelosti i bezbjednosti informacionih sistema.

Informaciona bezbjednost

Informaciona bezbjednost predstavlja zaštitu informacija i informacionih sistema od neovlašćenog pristupa, korišćenja, otkrivanja, poremećaja, izmjene ili uništenja. Cilj je osigurati **povjerljivost, integritet i dostupnost** informacija.

Ona obuhvata sve mjere koje omogućavaju organizaciji da upravlja rizicima, spriječi prijetnje, otkrije ih, dokumentuje i reaguje na njih. Na taj način organizacija štiti svoju IT infrastrukturu i podatke od neovlašćenih korisnika.

Važno je napomenuti da je informaciona bezbjednost povezana, ali različita od **cyber bezbjednosti**, koja se fokusira na zaštitu informacija od cyber napada, često sa vanjskih izvora. Cyber bezbjednost uključuje strategije, politike i standarde za zaštitu i operacije u digitalnom prostoru, te obuhvata smanjenje prijetnji, odgovore na incidente, otpornost sistema i obezbjeđenje informacija. Dok su mnogi principi informacione bezbjednosti primjenljivi na cyber bezbjednost, u ovom poglavlju fokus je na **politikama, procedurama i praksama informacione bezbjednosti** koje organizacija treba da implementira.

Fundamentalni aspekt informacione bezbjednosti su tri osnovna principa:

- **Povjerljivost** – osiguranje da informacije mogu vidjeti i koristiti samo ovlašćene osobe. Gubitak povjerljivosti znači da su informacije otkrivene neovlašćenim osobama.
- **Integritet** – zaštita informacija od neovlašćenih izmjena ili uništenja, uključujući osiguranje autentičnosti i neodricanja podataka. Gubitak integriteta je neovlašćena modifikacija ili uništenje informacija.
- **Dostupnost** – osiguranje da sistemi, podaci i aplikacije budu dostupni korisnicima kada su potrebni za obavljanje poslovnih aktivnosti. Gubitak dostupnosti znači da pristup informacijama ili sistemu nije moguć ili je poremećen.

Informaciona bezbjednost nije sama sebi svrha – ona je alat koji omogućava organizaciji da ostvari svoje ciljeve. To znači da treba štititi podatke, ali i omogućiti pristup informacijama onima kojima su potrebne za obavljanje poslova, uz prihvatljiv nivo rizika. Kontrola pristupa je ključna: korisnici smiju pristupati samo resursima i uslugama kojima su ovlašćeni, dok kvalifikovani korisnici ne smiju biti uskraćeni za pristup informacijama koje im trebaju.

U svojoj suštini, informaciona bezbjednost se bavi minimiziranjem izloženosti rizicima kroz sve djelove IT upravljanja. Neuspjeh u jednoj oblasti može ugroziti cijelu organizaciju. Čak i kada je poznato da je efektivno upravljanje rizicima ključno, rizici se često zanemaruju ili mjere zaštite nijesu ažurirane kako se mijenjaju uslovi.

Informaciona bezbjednost postaje sve važnija, posebno za državne i velike organizacije. Povezivanje mreža i dijeljenje informacija povećava složenost kontrole pristupa i zaštite podataka. Informacioni sistemi su kompleksni – oni povezuju tehnologiju, procese i ljude kako bi omogućili obradu, skladištenje i prenos informacija za podršku poslovnim ciljevima.

Cilj programa informacione bezbjednosti je smanjiti rizik od gubitka povjerljivosti, integriteta i dostupnosti informacija na prihvatljiv nivo. Bez takvog programa, organizacija je izložena riziku od:

- kršenja zakona i propisa;
- finansijskih gubitaka, kazni, smanjene prodaje ili troškova obnove;
- smanjenja efikasnosti i efektivnosti projekata i usluga;
- gubitka ili krađe računarskih resursa i imovine;
- neovlašćenog pristupa, otkrivanja ili uništenja osjetljivih informacija;
- hakerskih napada i potencijalnih zahtjeva za otkupninom;
- poremećaja kritičnih operacija;
- štete u reputaciji ili finansijama organizacije;
- zloupotrebe IT resursa za neovlašćene svrhe ili napade na druge sisteme;
- oštećenja mreža i opreme.

Potencijalna šteta može nastati usljed sljedećih situacija:

- **Povreda bezbjednosnih pravila i sistema zaštite** – bilo kakvo narušavanje postavljenih kontrola (npr. neovlašćen pristup sistemu, curenje podataka, zaobilaženje procedura).
- **Neovlašćeno povezivanje sa spoljnjim lokacijama** – uspostavljanje komunikacije ili razmjene podataka sa mrežama, serverima ili cloud servisima koji nijesu pod kontrolom

organizacije (npr. prikrivena veza malvera sa komandnim serverom ili slanje dokumenata na privatni Dropbox).

- **Izlaganje povjerljivih informacija zbog socijalnog inženjerstva** – manipulacija zaposlenih kako bi dobrovoljno otkrili pristupne podatke ili osjetljive informacije (npr. phishing, lažne IT podrške ili zahtjevi „pod hitno“ od navodnog menadžmenta).
- **Unutrašnje prijetnje** – situacije kada zaposleni zloupotrijebe svoja prava ili pristupne privilegije radi lične koristi ili nanošenja štete organizaciji.
- **Ranjivosti sistema na spoljnje napade** – tehničke slabosti u sistemu koje napadači mogu iskoristiti za upad, krađu podataka ili ometanje rada sistema.Takođe, upotreba društvenih mreža od strane organizacija donosi dodatne izazove za zaštitu podataka i privatnosti. Politike i procedure moraju regulisati pristup i korišćenje ličnih informacija, te upravljanje rizicima u ovim okruženjima.

Ključ uspjeha programa informacione bezbjednosti je **stvaranje organizacione kulture koja cijeni bezbjednost**. Ovo uključuje:

- Podizanje svijesti o bezbjednosti – kroz edukativne sesije i kontinuiranu obuku zaposlenih, od početka zaposlenja do odlaska iz organizacije.
- Posvećenost rukovodstva – rukovodstvo treba aktivno podržavati program i preuzeti odgovornost za informacione bezbjednosti. Bez iskrene podrške, zaposlenima je teško razviti osjećaj obaveze.
- Koordinacija kroz međufunkcionalne timove – timovi sa članovima iz više odjeljenja podstiču komunikaciju, saradnju i smanjuju dupliranje napora.

Kultura informacione bezbjednosti treba da obuhvata:

- Poravnanje sa poslovnim ciljevima – bezbjednost treba da podržava, a ne koči poslovne aktivnosti.
- Ravnotežu između ljudi, procesa, tehnologije i organizacije – svaki element mora funkcionisati zajedno da bi bezbjednost bila efektivna.
- Upravljanje rizicima – odluke o bezbjednosti treba da se donose vođene analizom rizika, što uključuje:

    1. Dodjelu odgovornosti višim rukovodiocima;
    2. Kontinuirano praćenje i razumijevanje rizika;
    3. Definisanje i komuniciranje tolerancije na rizik;
    4. Odgovornost rukovodstva za odluke i implementaciju programa upravljanja rizicima.

Informaciona bezbjednost u organizaciji obuhvata **12 osnovnih elemenata** (WGITA-IDI, 2022):

1. Procjena rizika
2. Politika bezbjednosti
3. Organizacija IT bezbjednosti
4. Operacije i upravljanje zapisima

5. Upravljanje imovinom
6. Bezbjednost ljudskih resursa
7. Fizička bezbjednost
8. Kontrola pristupa
9. Razvoj IT sistema, nabavka i održavanje
10. Upravljanje incidentima IT bezbjednosti
11. Upravljanje kontinuitetom poslovanja
12. Usaglašenost.

Svaki od ovih domena pomaže organizaciji da zaštiti svoje informacije i IT infrastrukturu, smanji rizike i osigura kontinuitet poslovanja.

Procjena rizika je proces identifikacije, analize i evaluacije rizika koji mogu uticati na informacioni sistem i resurse organizacije. Ona uključuje razmatranje:

- sve imovine i procesa povezanih sa sistemom;
- vanjskih i outsourcanih okruženja povezanih sa sistemom;
- potencijalnih prijetnji koje mogu ugroziti povjerljivost, integritet ili dostupnost informacija;
- ranjivosti sistema i njihovih potencijalnih posljedica;
- zahtjeva za zaštitom i mjera za ublažavanje rizika;
- odabira odgovarajućih sigurnosnih kontrola i analize odnosa rizika.

Nepravilno izvršena procjena rizika može dovesti do nedovoljne zaštite osjetljivih podataka, ili prekomjerne, nepotrebne zaštite.

Proces procjene rizika uključuje četiri koraka:

1. Priprema – razvoj organizacionog okvira za procjenu rizika.
2. Sprovođenje procjene – uključuje:
    - identifikaciju izvora prijetnji i događaja,
    - identifikaciju ranjivosti i predisponirajućih uslova,
    - procjenu vjerovatnoće pojave prijetnji,
    - procjenu potencijalnog uticaja,
    - određivanje ukupnog rizika na osnovu prethodnih analiza.
3. Komuniciranje rezultata – rezultati procjene se dijele relevantnim učesnicima i rukovodstvu.
4. Održavanje procjene – procjene rizika se ne rade jednokratno; potrebno ih je redovno ažurirati kako bi odražavale promjene u sistemu i okruženju.

Procjena rizika pomaže rukovodstvu da odabere odgovarajuće kontrole koje efektivno smanjuju rizik. Postoje tri nivoa potencijalnog uticaja:

- Nizak uticaj – ograničen negativan efekat na operacije, imovinu ili pojedince.
- Umjeren uticaj – ozbiljan negativan efekat na operacije, imovinu ili pojedince.
- Visok uticaj – težak ili katastrofalan negativan efekat na operacije, imovinu ili pojedince.

Ova kategorizacija utiče na rigoroznost testiranja bezbjednosnih kontrola, posebno kod sistema visokog rizika, gdje testovi mogu uključivati simulacije napada i procjenu efikasnosti zaštitnih mjera.

Politika bezbjednosti je skup pravila, standarda i procedura koje organizacija uspostavlja da bi regulisala način upravljanja, zaštite i distribucije resursa. Politika:

- definiše ciljeve i opseg bezbjednosti informacija, uključujući povjerljivost, integritet i dostupnost podataka;
- precizira odgovornosti zaposlenih i kriterijume za dodjelu ovlašćenja;
- određuje način korišćenja IT resursa, e-pošte, interneta i pristupa informacijama;
- opisuje procedure za backup, upravljanje zlonamjernim softverom, prijavu i reagovanje na incidente, te planove kontinuiteta poslovanja;
- uključuje mjere fizičke bezbjednosti, obuku zaposlenih i svijest o bezbjednosti;
- definiše proces upravljanja zakrpama (ispravke ranjivosti softvera) i metode komunikacije politike unutar organizacije.

Dobra politika bezbjednosti omogućava zaposlenima jasno razumijevanje svojih odgovornosti i olakšava organizaciji da zaštiti informacije bez ometanja svakodnevnih poslovnih aktivnosti.

Organizacija IT bezbjednosti podrazumijeva primjenu politike bezbjednosti unutar organizacije. Odgovornost za implementaciju politike može biti dodijeljena posebnoj jedinici ili pojedincu, koji zatim sarađuje sa svim djelovima organizacije kako bi se osigurali odgovarajući alati, procesi i resursi za njenu efikasnu primjenu.

Nakon implementacije politike, organizacija mora:

- obezbijediti obuku za zaposlene, kako bi razumjeli svoje obaveze i postupke u vezi sa bezbjednošću;
- reagovati na incidente bezbjednosti u skladu sa definisanim procedurama;
- osigurati da podaci kojima se pristupa unutar organizacije ili koji se dijele sa vanjskim partnerima budu odgovarajuće zaštićeni.

Revizor IT sistema ima zadatak da provjeri da li vanjske organizacije koje rukovode podacima mogu primijeniti zahtjeve bezbjednosti u skladu sa politikom organizacije.

Upravljanje operacijama i zapisima obuhvata procese i procedure koje organizacija koristi za svoje poslovne operacije sa fokusom na informacije i medije koji se koriste u tim operacijama. Ovo uključuje:

- organizacione procedure za ispravnu obradu podataka;
- dokumentovanje metoda za rukovanje medijima (nosiocima podataka) i podacima;
- procedure za hitne slučajeve;
- procedure za rezervne kopije (bekap) podataka;
- procedure za sigurnosti mreže.

Cilj je osigurati tačnost, sigurnost i dostupnost informacija u svim fazama njihovog korišćenja.

Upravljanje sredstvima predstavlja sistematski proces nadzora, održavanja, nadogradnje i odlaganja resursa koji imaju vrijednost za organizaciju.

Za IT, to uključuje:

- Oprema – održavanje tačnog inventara računara, servera, mrežne opreme i dodatnih uređaja;
- Softver – praćenje licenci, verzija i instalacija;
- Podaci i dokumentacija – zaštita i čuvanje informacija i dokumentacije;
- Sigurnost – fizička zaštita opreme, zaključavanje prostorija i kontrola pristupa.

Upravljanje IT sredstvima je ključno jer nepotpuni inventar može dovesti do toga da:

- organizacija ne primjenjuje odgovarajuće kontrole bezbjednosti na sve resurse;
- otežava planiranje i nadogradnju softvera i hardvera u skladu sa budućim poslovnim potrebama;
- povećava rizik od gubitka ili neovlašćenog pristupa resursima.

Efikasno upravljanje sredstvima omogućava organizaciji da sigurno i ekonomično koristi svoje IT resurse, smanjujući rizik i osiguravajući kontinuitet poslovanja.

Kada je riječ o **sigurnosti ljudskih resursa**, zaposleni koji rukovode ličnim ili osjetljivim podacima u organizaciji moraju dobiti odgovarajuću obuku i redovna ažuriranja, kako bi se osigurala zaštita informacija koje su im povjerene. Svaka radna pozicija treba imati jasno definisane uloge i odgovornosti, dokumentovane u skladu sa politikom bezbjednosti organizacije. Podaci organizacije moraju biti zaštićeni od neovlašćenog pristupa, otkrivanja, modifikacije, uništenja ili ometanja. Upravljanje rizicima ljudskih resursa i privatnosti je potrebno u sve tri faze zaposlenja.

Tri ključna područja sigurnosti ljudskih resursa su:

1. Prije zaposlenja (Pre-employment)
    - Definisanje uloga i odgovornosti za svaku radnu poziciju.
    - Određivanje pristupa osjetljivim informacijama prema potrebama posla.
    - Procjena kandidata kroz odgovarajući nivo provjere (screening) u skladu sa IT politikom organizacije.
    - U ovoj fazi se takođe definišu i uslovi ugovora o radu.
2. Tokom zaposlenja (During employment)
    - Zaposleni koji imaju pristup osjetljivim informacijama treba da dobijaju periodične podsjetnike svojih obaveza.
    - Obuka o bezbjednosti i svijest o prijetnjama treba da se stalno ažurira, kako bi zaposleni razumjeli aktuelne rizike i sigurnosne procedure za njihovo ublažavanje.
3. Po prestanku zaposlenja (Termination of employment)
    - Pristup osjetljivim informacijama mora biti odmah ukinut po prestanku radnog odnosa.
    - Svi resursi organizacije koji su bili kod zaposlenog (računari, kartice, dokumenti) moraju biti vraćeni.

- Preporučuje se priprema posebnog formulara za dokumentovanje obavljenog posla, provjere da je pristup ukinut i da su svi resursi vraćeni.

Program svijesti o bezbjednosti treba biti stalno aktivan u organizaciji, podsjećajući sve zaposlene na moguće rizike i odgovornosti koje imaju kao čuvari informacija organizacije.

Fizička bezbjednost odnosi se na mjere koje sprečavaju neovlašćenim osobama pristup zgradama, postrojenjima, opremi ili pohranjenim informacijama. To uključuje i dizajn objekata koji je otporan na potencijalne neprijateljske radnje. Primjeri mjera mogu biti jednostavni, poput zaključanih vrata, ali i složeni, uključujući višeslojne barijere, čuvare, stražarske kućice i sofisticirane sisteme nadzora.

Primarna svrha fizičke bezbjednosti je ograničavanje fizičkog pristupa neovlašćenim osobama, ali postoje i druge situacije u kojima su mjere korisne, kao što su:

- Ograničavanje pristupa unutar postrojenja ili određenim resursima;
- Primjena fizičkih kontrola za smanjenje rizika od fizičkih incidenata, poput požara, poplava ili drugih prirodnih nepogoda.

Važno je napomenuti da bezbjednost nikada nije apsolutna – ona može smanjiti rizike, ali ih ne može potpuno eliminisati. Zato se primjenjuje princip „obrane u dubini“, gdje se koristi kombinacija preklapajućih i komplementarnih kontrola.

Primjeri kontrola fizičkog pristupa za zaštićena postrojenja uključuju:

- Obeshrabrivanje potencijalnih provalnika – npr. upozoravajući znakovi i oznake perimetra;
- Razlikovanje ovlašćenih od neovlašćenih osoba – npr. propusnice, ključevi, elektronski pristupni sistemi;
- Odlaganje i sprečavanje provale – npr. čvrsti zidovi, kvalitetne brave, sefovi;
- Otkrivanje i praćenje provala – npr. alarmni sistemi i video-nadzor;
- Reagovanje na incidente – npr. angažovanje čuvara ili policije.

Fizičke kontrole se posebno odnose na prostorne jedinice sa koncentracijom IT resursa, kao što su:

- centri podataka;
- prostorije sa velikim računarima ili serverima;
- komunikacijske prostorije.

Nedostatak ovih kontrola, posebno u zahtjevnim okruženjima, može značajno uticati na dostupnost sistema i opreme koja je neophodna za obavljanje poslovnih funkcija i podršku misiji organizacije.

Kontrola pristupa odnosi se na ograničavanje i upravljanje time ko smije pristupiti određenom resursu i pod kojim uslovima. Resurs može biti fizička lokacija (npr. zgrada, server prostorija) ili digitalni sistem (npr. baza podataka, mrežni servis, aplikacija). Kontrola može biti **fizička** (brave, kartice za pristup) ili **logička** / **digitalna** (korisnička imena, lozinke, autentifikacija, mrežni protokoli).

Kontrola pristupa omogućava organizaciji da zaštiti povjerljive informacije, sisteme i opremu, i obuhvata sljedeće aspekte:

- Izdavanje i upravljanje identitetima i kredencijalima (pristupnim podacima) – definisanje ko je ovlašćeni korisnik, izdavanje pristupnih naloga, njihova verifikacija, revizija i opoziv kada pristup više nije potreban;
- Fizička kontrola pristupa sredstvima – zaključana oprema, kontrolisani ulazi, nadzor;
- Upravljanje daljinskim pristupom – ako se koristi rad na daljinu ili VPN, pristup mora biti kontrolisan i nadziran;
- Dodjela dozvola prema principu najmanjih privilegija – korisnici treba da imaju samo onaj nivo pristupa koji je neophodan za obavljanje posla, ništa više;
- Razdvajanje dužnosti – kako bi se spriječile zloupotrebe, ključne funkcije se raspoređuju među više osoba (npr. jedna odobrava transakciju, druga je izvršava);
- Zaštita integriteta mreže – segmentacija mreže i ograničavanje pristupa određenim mrežnim zonama;
- Autentifikacija korisnika i uređaja – primjena jedno-faktorske ili više-faktorske autentifikacije, zavisno od rizika i osjetljivosti podataka.

Procjena rizika i tolerancija organizacije na rizik određuju koji nivo kontrole pristupa je potreban. Što je resurs osjetljiviji, kontrole moraju biti strože.

U organizacijama koje obrađuju osjetljive ili lične podatke (posebno u javnoj upravi, zdravstvu, finansijama), kontrola pristupa je ključna kako bi se osiguralo da samo ovlašćena lica imaju uvid u određene informacije, čime se štiti privatnost i sprečavaju sigurnosni incidenti.

Kada organizacija **razvija ili nabavlja IT sisteme**, proizvode ili usluge, važno je da prepozna i kontroliše rizike koji mogu nastati u lancu snabdijevanja. Lanac snabdijevanja obuhvata sve faze – od dizajna i razvoja, preko proizvodnje i rukovanja, pa sve do isporuke i korišćenja proizvoda od strane krajnjeg korisnika.

S obzirom na to da je u ove procese često uključeno više vanjskih dobavljača i podizvođača, upravljanje rizicima u lancu snabdijevanja postaje kritična funkcija organizacije, posebno kada je riječ o cyber bezbjednosti.

Cilj upravljanja rizicima u IT lancu snabdijevanja je da se na vrijeme identifikuju i ublaže prijetnje kao što su:

- Uvođenje zlonamjerne funkcionalnosti u proizvod,
- Krivotvoreni ili neovlašćeno izmijenjeni proizvodi,
- Ranjivosti nastale lošim razvojnim ili proizvodnim praksama kod dobavljača.

Kako bi to postigla, organizacija bi trebalo da primijeni sljedeće mjere:

- Definisanje zahtjeva cyber bezbjednosti za dobavljače,
- Ugradnja tih zahtjeva u ugovore i druge formalne sporazume,
- Jasna komunikacija sa dobavljačima o načinu verifikacije ispunjenosti bezbjednosnih zahtjeva,
- Provjera i evaluacija ispunjenosti zahtjeva (npr. kroz izvještaje bezbjednosnih operativnih centara ili formalne revizije),
- Kontinuirani nadzor i dokumentovanje ovih aktivnosti.

Nakon što je IT sistem razvijen ili nabavljen, on ne ostaje statičan — potrebno ga je **kontinuirano održavati** tokom cijelog životnog ciklusa. To uključuje:

- instaliranje ažuriranja i zakrpa (patch-ispravka grešaka ili bezbjednosnih propusta u softveru),
- otklanjanje grešaka u radu sistema,
- adaptaciju sistema na nove poslovne potrebe ili integraciju s drugim platformama.

Upravljanje zakrpama predstavlja proces koji obuhvata:

1. identifikaciju dostupnih zakrpa,
2. preuzimanje i testiranje,
3. instalaciju,
4. verifikaciju da je zakrpa ispravno primijenjena.

Zakrpe su posebno važne sa sigurnosnog aspekta jer zatvaraju ranjivosti koje napadači mogu iskoristiti. Pravovremena primjena zakrpa značajno smanjuje rizik od kompromitacije sistema.

Upravljanje incidentima obuhvata procese i prakse kojima se osigurava da su incidenti ili greške registrovani, analizirani i riješeni pravovremeno. U kontekstu cyber bezbjednosti, upravljanje incidentima IT bezbjednosti podrazumijeva nadzor i otkrivanje bezbjednosnih događaja u IT sistemima i mrežama (npr. pokušaj neovlašćenog pristupa, malver/virus), te preduzimanje odgovarajućih mjera kao reakciju na te događaje. To je specijalizovana forma upravljanja incidentima fokusirana na zaštitu informacija i infrastrukture.

Organizacije treba da uspostave formalan proces, plan i politiku reagovanja na incidente. Tipičan proces reagovanja na incidente sastoji se iz četiri faze:

- Priprema – uspostavljanje i obuka tima za reagovanje na incidente, definisanje procedura, obezbjeđivanje alata i resursa, te preventivno jačanje sigurnosti sistema primjenom kontrola zasnovanih na procjeni rizika.
- Otkrivanje i analiza – identifikacija potencijalnog incidenta korišćenjem alata kao što su IDS/IPS sistemi (sistemi za otkrivanje i prevenciju upada), antivirusni programi, analizatori logova ili prijave korisnika. Nakon otkrivanja, incident se analizira i verifikuje prema unaprijed definisanom postupku, uz dokumentovanje svih aktivnosti.
- Suzbijanje, eliminacija i oporavak – ograničavanje širenja incidenta (npr. isključenjem sistema ili mrežne veze), uklanjanje uzroka incidenta poput zlonamjernog softvera ili kompromitovanih naloga, te vraćanje sistema u normalno stanje (npr. vraćanjem bekapa, ponovnom instalacijom, promjenom lozinki i primjenom zakrpa).
- Aktivnosti nakon incidenta – analiza iskustva, čuvanje relevantnih dokaza i revizija procesa reagovanja kako bi se unaprijedila buduća praksa. Ovo uključuje sesije sa naučenim lekcijama i dokumentovanje preporuka za poboljšanje.

Planiranje kontinuiteta poslovanja predstavlja proces u kojem organizacija unaprijed definiše kako će održati ili obnoviti svoje ključne poslovne procese nakon prekida u radu. Takođe obuhvata planiranje funkcionisanja organizacije u otežanim uslovima (npr. prirodne katastrofe, tehnički kvarovi, napadi na sisteme) (vidi prethodnu sekciju).

IS revizor treba da provjeri i procijeni **usklađenost** sa svim internim i eksternim zahtjevima, uključujući zakonske, regulatorne, sigurnosne, ekološke i druge obaveze koje utiču na rad i sigurnost informacija u organizaciji.

Politike i procedure IT bezbjednosti, zajedno s njihovom primjenom, omogućavaju organizaciji zaštitu IT infrastrukture od neovlašćenih korisnika. IT politika organizacije postavlja visoke standarde koje zaposleni i organizacija moraju poštovati kako bi zaštitili kritična sredstva. Takođe, ona osigurava obuku zaposlenih, pridržavanje procedura za pristup i kontrolu podataka, te usklađenost s važećim zakonima i propisima.

Implementacija efikasnog sistema bezbjednosti informacija suočava se s mnogim izazovima. Bez adekvatnog upravljanja ovim preprekama, organizacija je izložena povećanom riziku od neuspjeha u ostvarivanju svojih ciljeva. Svaka organizacija ima jedinstvene izazove zbog faktora vezanih za radno okruženje, kao i zbog političkih, geografskih, ekonomskih i socijalnih specifičnosti, a revizor je odgovoran da ukaže menadžmentu na **rizike bezbjednosti informacija.**

Primjeri značajnih rizika su (WGITA-IDI, 2022):

- neovlašćeno otkrivanje informacija
- neovlašćena modifikacija ili uništenje informacija
- napad na informacioni sistem (npr. hakerski napad, virus)
- uništenje infrastrukture informacionog sistema
- poremećaj pristupa ili korišćenja informacija ili sistema
- poremećaj obrade informacionog sistema
- krađa informacija ili podataka.

Posebna područja pažnje prilikom procjene rizika su (WGITA-IDI, 2022):

- strategije bezbjednosti koje nijesu usklađene s IT ili poslovnim zahtjevima
- neujednačena primjena politika na različitim nivoima organizacije
- neusklađenost sa internim i eksternim zahtjevima
- bezbjednost informacija koja nije uključena u održavanje i razvoj projekata
- dizajn arhitekture koji dovodi do neefikasnih ili pogrešno usmjerenih rješenja
- nedostatak fizičke bezbjednosti i slab nadzor nad sredstvima
- neadekvatna konfiguracija hardverskih sistema
- nejasna struktura odgovornosti za bezbjednost informacija
- slabosti u rješenjima ljudskih resursa
- neefikasno korišćenje finansijskih resursa namijenjenih bezbjednosti
- bezbjednost informacija koja se ne prati ili se prati neefikasno.

Revizija bezbjednosti informacija zahtijeva fokus na svih 12 elemenata informacione bezbjednosti. Revizor treba da procijeni adekvatnost metoda procjene rizika i da analizira implementaciju bezbjednosnih kontrola. Mreža revizijskih pitanja pomaže u definisanju kriterijuma evaluacije, potrebne dokumentacije i tehničke analize. Na kraju, revizor razvija detaljan revizorski program prema potrebama i nalazima prilikom terenskog rada.

Sažet pregled svih 12 elemenata informacione bezbjednosti je dat u Tabeli 4.

Tabela 4. Elementi informacione bezbjednosti

Element	**Opis / Svrha**	**Ključne aktivnosti / mjere**	**Primjeri**
Procjena rizika	Identifikacija i evaluacija rizika	Identifikacija prijetnji, ranjivosti, procjena uticaja	Analiza uticaja napada na server
Politika bezbjednosti	Definiše pravila i smjernice za zaštitu resursa	Pravila pristupa, procedure, svijest o bezbjednosti	Politika lozinki, procedure rezervnih kopija
Organizacija IT bezbjednosti	Implementacija i praćenje politike	Obuka zaposlenih, delegiranje odgovornosti	IT sigurnosni tim, plan reagovanja na incidente
Operacije i upravljanje zapisima	Praćenje i vođenje evidencije operacija	Dokumentovanje procedura, sigurnosne kopije, logovi	Evidencija pristupa sistemima, backup podataka
Upravljanje sredstvima	Praćenje i zaštita IT resursa	Inventar opreme, softvera, podataka	Inventar računara, praćenje licenci
Bezbjednost ljudskih resursa	Upravljanje sigurnošću tokom zaposlenja	Obuka, definisanje uloga, kontrola pristupa	Pristup osjetljivim podacima, opoziv kredencijala
Fizička bezbjednost	Zaštita od fizičkog pristupa i oštećenja	Ograde, kontrole pristupa, okolišne mjere	Alarmni sistemi, protivpožarna zaštita
Kontrola pristupa	Upravljanje pristupom resursima	Autentifikacija, autorizacija, segmentacija mreže	PIN, biometrija, kredencijali
Razvoj, nabavka i održavanje IT sistema	Siguran razvoj i održavanje IT	Upravljanje rizicima lanca snabdijevanja, zakrpe	Ažuriranje softvera, instalacija zakrpa
Upravljanje incidentima	Otkrivanje i reagovanje na sigurnosne događaje	Detekcija, analiza, oporavak, lekcije naučene	Virus, hakerski napad, neovlašćen pristup
Upravljanje kontinuitetom poslovanja	Planiranje i obnova poslovnih procesa	Planovi oporavka, testiranje kontinuiteta	Rezervni serveri, alternativne lokacije
Usaglašenost	Praćenje poštovanja propisa i standarda	Interna i eksterna revizija	Poštovanje zakona o zaštiti podataka, ISO standardi

1.3. Vrste informacionih sistema

Informacioni sistemi (IS) predstavljaju srž svakog modernog poslovanja i državne administracije, jer omogućavaju prikupljanje, obradu, čuvanje i korišćenje podataka za donošenje odluka i vođenje poslovnih procesa. IS se mogu klasifikovati na više načina, a u ovom udžbeniku prihvatamo osnovnu podjelu na **operativne** i **upravljačke** sisteme (O'Brien & Marakas, 2011).

Operativni informacioni sistemi primarno podržavaju svakodnevno funkcionisanje organizacije. Njihova uloga je da obezbijede efikasno procesiranje poslovnih transakcija, praćenje i automatizaciju poslovnih procesa, kao i omogućavanje komunikacije i saradnje među zaposlenima. Ključni predstavnici ove kategorije su **sistemi za procesiranje transakcija (Transaction Processing Systems – TPS)**. Oni čuvaju i obrađuju podatke nastale tokom poslovnih aktivnosti, kao što su prodaja, nabavka, računovodstvo ili upravljanje zalihama. Ovi sistemi mogu raditi u batch režimu, gdje se podaci akumuliraju i obrađuju periodično (npr. noću ili krajem mjeseca), ili u real-time (online) režimu, gdje se podaci obrađuju odmah tokom same transakcije. Primjer za online obradu podataka su POS (point-of-sale) sistemi u prodajnim objektima, gdje se podaci o kupovini automatski šalju centralnom računaru u trenutku obavljanja prodaje.

Upravljački informacioni sistemi pružaju podršku menadžmentu na svim nivoima, od operativnog do strateškog. **Management Information Systems (MIS)** obezbjeđuju unaprijed definisane izvještaje na osnovu podataka iz operativnih baza. Za razliku od TPS sistema, MIS izvještaji obično ne prikazuju pojedinačne transakcije, već su podaci klasifikovani i agregirani, što znači da su grupisani i sumirani unutar grupa, tako da menadžeri mogu brzo uočiti trendove i donijeti odluke kod strukturiranih problema odlučivanja (gdje su koraci i pravila unaprijed jasno definisani). Na primjer, menadžer prodaje može koristiti MIS izvještaj o prodaji proizvoda u prethodnom mjesecu kako bi odlučio o količini narudžbi za naredni mjesec.

Za rješavanje polustrukturiranih i nestrukturiranih problema (gdje potrebni podaci nijesu uvijek unaprijed jasni ili pravila odlučivanja nijesu potpuno definisana), koriste se **Decision Support Systems (DSS)**. DSS sistemi omogućavaju menadžerima da analiziraju podatke i simuliraju različite scenarije, često koristeći specijalizovane **višedimenzionalne baze podataka (Data Warehouse)**, gdje su podaci o poslovnim činjenicama (kao što je na primjer iznos nabavke) organizovani po više različitih dimenzija (npr. proizvod, vrijeme, dobavljač). Ovi sistemi podržavaju interaktivnu, ad hoc analizu i omogućavaju korisnicima da unose nove podatke, mijenjaju pretpostavke i vrše „what-if" simulacije. Ad hoc analiza znači da model za analizu korisnik može kreirati po potrebi. What-if simulacije omogućavaju ispitivanje „šta bi se desilo ako", različite promjene koje nastupe u poslovnom procesu (Kašćelan, 2016).

Posebnu kategoriju DSS sistema čine **inteligentni – sugestivni sistemi**, koji primjenjuju tehnike vještačke inteligencije, uključujući mašinsko učenje i neuronske mreže, kako bi automatski generisali sugestije za nestrukturirane probleme odlučivanja. Neki inteligentni sistemi, poput data mining rješenja, analiziraju velike baze podataka i otkrivaju skrivene obrasce i prediktivne informacije, što danas predstavlja veoma popularnu primjenu u poslovanju i javnoj upravi (Kašćelan, 2016).

Za izvršni nivo menadžmenta koriste se **Executive Information Systems (EIS)**, koji pružaju kritične informacije u jednostavnom i preglednom formatu. Ovi sistemi mogu automatski upozoravati na potencijalno kritične situacije. Na primjer, menadžer prodaje može pratiti dnevne rezultate po prodajnim mjestima i, kada prodaja padne ispod definisane granice dobiti, upozorenje u vidu paljenja crvene lampice ili upadljivog zvučnog signala.

Savremeni informacioni sistemi sve više integrišu elemente vještačke inteligencije, automatizaciju i velike podatke, što omogućava brže i preciznije donošenje odluka, kao i efikasnije upravljanje resursima. Za revizore, poznavanje razlika i primjena ovih sistema je ključno, jer im omogućava da procijene tačnost, sigurnost i pouzdanost informacija koje menadžment koristi u odlučivanju.

1.4. Informacioni sistemi i moderne tehnološke platforme

Savremeni informacioni sistemi danas se oslanjaju na moćne tehnološke platforme koje omogućavaju obradu velikih količina podataka, automatizovane odluke, rad na daljinu i visoku dostupnost usluga građanima. Ove platforme koje uključuju vještačku inteligenciju, velike podatke, računarstvo u oblaku, internet stvari i blockchain, sve više oblikuju način na koji državne institucije funkcionišu. One mijenjaju način pružanja javnih usluga i otvaraju nova pitanja za revizore – pitanja privatnosti, odgovornosti za podatke, upravljanja rizicima i transparentnosti.

Vještačka inteligencija (Artificial Intelligence – AI) i veliki podaci (Big Data)

Kroz istoriju razvoja računarske nauke čovjek je sve više pokušavao da prebaci dio mentalnog rada na mašine, ne samo u pogledu obrade podataka, već i donošenja odluka, prepoznavanja obrazaca i zaključivanja. Ta ambicija postepeno je izrodila polje poznato kao vještačka inteligencija. U najširem smislu, vještačka inteligencija predstavlja sposobnost računarskih sistema da obavljaju zadatke za koje se tradicionalno smatralo da zahtijevaju ljudsku inteligenciju: uočavanje, razumijevanje, zaključivanje, učenje iz iskustva i čak stvaranje novih sadržaja. Iako se u svakodnevnim razgovorima pojam AI često vezuje isključivo za moderne sisteme koji uče iz podataka, istorijski gledano, razvoj vještačke inteligencije tekao je u više grana i pravaca.

Jedan od najstarijih pristupa su takozvani ekspertni sistemi, koji su nastajali krajem 70-ih i početkom 80-ih godina. Ideja je bila da se znanje stručnjaka iz određene oblasti „uhvati“ u obliku pravila tipa ako-je-ovo-tada-uradi-ono, pa da računar može da imitira njihovo odlučivanje. Takvi sistemi imali su takozvanu bazu znanja i mehanizam zaključivanja koji je logičkim putem provjeravao pravila i donosio odluke. Njihova prednost bila je transparentnost – ljudski ekspert je mogao da razumije kako je sistem došao do zaključka. Međutim, ovi sistemi su zavisili od unaprijed definisanih pravila, što znači da nijesu mogli učiti iz novih primjera, a održavanje ogromnih baza pravila postajalo je sve teže. Ipak, mnoge javne institucije i danas imaju ostatke ekspertnih sistema u vidu automatizovanih pravila za donošenje odluka, na primjer, kod procedura za automatsko odobravanje dokumenata, obračun poreza ili provjeru validnosti zahtjeva građana.

Za razliku od ekspertnih sistema, savremeni **AI sistemi**, posebno oni zasnovani na mašinskom učenju, ne dobijaju pravila unaprijed, već ih otkrivaju analizom velikog broja primjera iz realnog svijeta. **Mašinsko učenje** predstavlja skup metoda koje omogućavaju računaru da iz podataka nauči strukture, obrasce i zakonitosti, i da zatim te obrasce koristi za donošenje odluka ili

pravljenje predikcija. Unutar mašinskog učenja postoje brojne tehnike, kao što su stabla odlučivanja, neuronske mreže, algoritmi zasnovani na statističkoj analizi ili metodama klasterizacije. Stabla odlučivanja, na primjer, imitiraju način donošenja odluka kroz niz pitanja koja vode do konačnog zaključka. Neuronske mreže, inspirisane načinom funkcionisanja ljudskog mozga, koriste slojeve međusobno povezanih jedinica koje obrađuju informacije i prilagođavaju svoje veze tako da vremenom sve preciznije odgovaraju na zadatke. Posebno su zanimljive duboke neuronske mreže, koje imaju veliki broj slojeva i sposobne su da izuzetno dobro prepoznaju kompleksne obrasce – od prepoznavanja lica na snimcima, do automatskog prevođenja jezika ili generisanja teksta (Kašćelan, 2016).

Obrazovanje o vještačkoj inteligenciji postaje sve važnije, jer omogućava pojedincima i organizacijama da razumiju potencijal i ograničenja ove tehnologije, da procijene rizike i da je odgovorno primjenjuju. Posebno u državnim organima, gdje odluke mogu imati širok društveni uticaj, razumijevanje AI pomaže u donošenju informisanih odluka, unapređuje efikasnost rada i olakšava inovacije u javnim uslugama.

Finska je 2018. godine pokrenula kurs „Elements of AI“, besplatne onlajn kurseve osmišljene da uvedu osnovne koncepte vještačke inteligencije osobama koje nijesu stručnjaci u toj oblasti. Kursevi sadrže materijale za samostalno učenje, interaktivni sadržaj i zadatke koji pomažu polaznicima da savladaju koncepte, metode upotrebe i ograničenja tehnologije. Finska vlada je obećala da će obrazovati najmanje jedan odsto stanovništva, cilj koji je brzo ostvaren i premašen. Kursevi su sada dostupni na više od 20 jezika, a oko milion ljudi širom svijeta ih je uspješno završilo. Slično tome, u Singapuru je pokrenut nacionalni program „AI for Everyone“, kojim vlada omogućava pojedincima i organizacijama da steknu vještine za primjenu vještačke inteligencije i mašinskog učenja u svrhu društvene koristi. Program nudi kurseve i radionice, kao i finansijsku podršku i savjetovanje za projekte koji doprinose društvenim promjenama. U Sjedinjenim Američkim Državama zakonodavstvo, koje predviđa uspostavljanje programa obuke o vještačkoj inteligenciji za federalne lidere, trenutno je u procesu razmatranja u Kongresu. Cilj ovog programa je pružiti smjernice za upotrebu AI, kako bi federalni lideri mogli pravilno procijeniti rizike i koristi ove tehnologije u skladu sa misijom svojih agencija i potrebama zajednici (Salesforce, 2025).

Uz klasično mašinsko učenje, posljednjih godina razvili su se i novi pravci kao što su **generativna vještačka inteligencija** i **kognitivni sistemi**. **Generativna AI** ima sposobnost da stvara nove sadržaje – tekstove, slike, muziku ili čak video-zapise – oponašajući stil i strukturu podataka na kojima je obučavana. Ovakvi sistemi, koji se oslanjaju na velike jezičke modele i kompleksne neuronske mreže, već se koriste za pripremu izvještaja, automatsko generisanje obrazaca, predloga rješenja u pravnim ili upravnim postupcima ili kao asistenti revizorima koji analiziraju obimnu dokumentaciju. Iako ove tehnologije donose ogromne mogućnosti, otvaraju i pitanja etike, odgovornosti i transparentnosti – posebno kada AI donosi preporuke koje mogu uticati na odluke javne uprave. Neki istraživači govore i o **kognitivnim AI sistemima**, koji ne samo da procesuiraju podatke, već pokušavaju da razumiju kontekst, namjeru i smisao, što je posebno važno za javne servise koji komuniciraju s građanima.

Upotreba generativne vještačke inteligencije u vladinim agencijama SAD-a rapidno se širi (Nazzaro, 2025). Broj primjena generativne AI u 11 saveznih agencija porastao je sa 32 slučaja u 2023. godini na 282 u 2024. godini. Agencije koriste ovu tehnologiju kako bi poboljšale pisanu

komunikaciju, povećale efikasnost pristupa informacijama i pratili napredak svojih programa. Najveći rast zabilježilo je Ministarstvo zdravstva i ljudskih usluga (HHS), sa 7 slučajeva u 2023. godini na 116 u 2024. godini. Ovaj primjer pokazuje koliko brzo generativna AI postaje važan alat u modernizaciji vladinih funkcija i unapređenju administrativnih procesa.

Razvoj AI snažno je povezan s pojavom velikih količina podataka, poznatih pod nazivom **Big Data**. Današnje društvo proizvodi ogromne količine digitalnih zapisa: državne službe bilježe zahtjeve korisnika, bolnički sistemi čuvaju medicinske nalaze, poreske uprave prate tokove prihoda i rashoda, saobraćajni sistemi generišu podatke o kretanju vozila, a komunikacione mreže bilježe svaki poziv, poruku ili elektronsku transakciju. Ovakvi podaci nijesu samo veliki po obimu, već i raznovrsni – neki su strukturirani u tabelama kao što su registri građana, drugi su nestrukturisani poput e-mailova, dokumenata ili audio-snimaka poziva ka službama. Karakteristično je i to da podaci dolaze velikom brzinom, u realnom vremenu, što zahtijeva posebne tehnologije obrade koje mogu brzo da detektuju promjene i donesu odluke u hodu. Zbog svega ovoga, big data se opisuje kroz nekoliko karakteristika: obim, brzinu, raznovrsnost i promjenljivost (Marz & Warren, 2015).

Iako big data pruža ogromne mogućnosti za poboljšanje javnih usluga, ona nosi i izazove. Samo skladištenje takvih količina podataka zahtijeva posebnu infrastrukturu, a njihova obrada traži algoritme koji mogu da funkcionišu i kada se ne zna unaprijed kako su podaci strukturisani. Poseban problem je zaštita privatnosti građana, jer analiza podataka može lako da dovede do identifikacije pojedinaca čak i kada su podaci formalno anonimizovani. Na primjer, ako država integriše baze podataka zdravstvenog sistema, poreske uprave i evidencije kretanja kroz elektronske granice, na osnovu kombinacije ovih informacija moguće je otkriti obrasce ponašanja pojedinaca. Zato revizori moraju da razumiju da velike baze podataka nijesu samo tehničko pitanje skladištenja, već i pravno pitanje zaštite privatnosti i kontrole pristupa.

Posebna vrijednost big data postaje vidljiva tek kada se na te podatke primijene AI metode. Na primjer, sistem za rano otkrivanje poreskih prevara može analizirati milione transakcija i otkriti protivrječnosti koje ljudsko oko nikada ne bi primijetilo. Algoritmi mogu da primijete da određena firma prijavljuje prihode koji odstupaju od prosjeka sličnih firmi u regionu, ili da građanin podnosi zahtjeve za socijalnu pomoć, a pritom se na osnovu drugih podataka vidi da posjeduje vozila visoke vrijednosti. Takve odluke ne donose sistemi sami, već generišu signale upozorenja koje zatim analiziraju nadležni službenici.

Za javne institucije, big data znači mogućnost da se uoče trendovi u potrošnji građana, prepoznaju rizične tačke u budžetskom trošenju, optimizuju tokovi rada ili povežu različiti državni registri radi bolje koordinacije između službi. Na primjer, povezivanjem baze zdravstvenog osiguranja, poreske evidencije i socijalnih davanja, može se otkriti zloupotreba prava ili dupliranje naknada. Međutim, analiza velikih podataka nosi i značajne rizike: privatnost građana mora biti zaštićena, podaci moraju biti anonimizovani tamo gdje je to potrebno, a rukovanje njima mora biti transparentno i u skladu sa zakonom.

Jedan od konkretnih primjera primjene vještačke inteligencije i velikih podataka u državnim institucijama dolazi iz indijske savezne države Tamil Nadu (The Times of India, 2025). Vlada je razvila centralizovanu bazu podataka koja sadrži stotine miliona anonimizovanih zapisa iz različitih vladinih programa, obuhvatajući oblasti kao što su poljoprivreda, zdravstvo, obrazovanje

i saobraćaj. Ovi podaci se dijele sa startapovima i tehnološkim firmama kako bi trenirali AI modele, omogućavajući identifikaciju obrazaca, unapređenje postojećih programa i dizajniranje efikasnijih politika. Ovaj pristup ne samo da poboljšava administrativnu efikasnost, već i doprinosi inovacijama u javnim uslugama.

Ako revizor razumije osnovne principe AI i Big Data, on može procijeniti da li institucija koristi podatke na odgovoran način i da li postoji rizik od zloupotreba, diskriminacije ili narušavanja privatnosti. Revizor ne mora biti programer, ali mora razumjeti logiku iza pojmova kao što su algoritamsko odlučivanje, skupovi za obuku modela i pristrasnost podataka, jer samo tako može prepoznati da li je odluka koju je sistem predložio zasnovana na provjerenim pravilima ili na statističkim korelacijama koje mogu biti pogrešno protumačene.

Cloud

Cloud tehnologija, ili računarstvo u oblaku, predstavlja model korišćenja računarskih resursa, poput servera, baza podataka, aplikacija ili prostora za skladištenje preko interneta, bez potrebe da organizacija posjeduje i održava sopstvenu fizičku infrastrukturu. Umjesto kupovine servera, instalacije softvera i zapošljavanja dodatnog tehničkog osoblja za održavanje, organizacije mogu da iznajme te resurse od provajdera oblaka i plaćaju ih po principu stvarne potrošnje. Ovo omogućava veću fleksibilnost, jer se kapacitet može brzo povećati ili smanjiti u zavisnosti od potreba, a sistemi mogu biti dostupni 24 časa dnevno, sa bilo koje lokacije.

U praksi, postoje različiti modeli cloud usluga. Najosnovniji nivo je **infrastruktura kao usluga (IaaS – Infrastructure as a Service)**, gdje organizacija iznajmljuje samo računske resurse – virtuelne servere, skladište i mrežnu infrastrukturu – i sama upravlja aplikacijama koje na njima pokreće. Na sljedećem nivou su **platforme kao usluga (PaaS – Platform as a Service)**, koje obezbjeđuju okruženje za razvoj i pokretanje aplikacija, gdje korisnik ne mora da brine o instaliranju operativnih sistema, baza ili programskih okvira. Najviši nivo je **softver kao usluga (SaaS – Software as a Service)**, gdje organizacija jednostavno koristi gotovu aplikaciju putem interneta, bez ikakve instalacije – kao što su sistemi za elektronsku poštu, upravljanje dokumentima ili državne platforme za elektronske dozvole i prijave (Erl, Puttini, & Mahmood, 2013).

Državne institucije sve češće prelaze na ovakve modele kako bi smanjile troškove održavanja, povećale sigurnost i osigurale veću dostupnost usluga građanima. Na primjer, platforme za elektronsku naplatu taksi, onlajn registraciju preduzeća, sistem elektronskih potpisivanja dokumenata ili digitalni katastar mogu biti hostovani u oblaku, što omogućava brže ažuriranje, veću otpornost na kvarove i jednostavniju integraciju između različitih državnih sistema. Globalni provajderi oblaka, kao što su Amazon (AWS), Microsoft Azure i Google Cloud, nude različite servise, uključujući naprednu analitiku, alate za obradu velikih podataka, sisteme za automatsku skalabilnost i čak unaprijed pripremljene modele vještačke inteligencije.

Na primjer, u julu 2025. godine, britanska vlada je sklopila strateški sporazum s Google Cloud-om kako bi modernizovala zastarjele tehnološke sisteme u javnim institucijama poput Nacionalne zdravstvene službe (NHS), lokalnih vijeća i drugih agencija. Ovaj korak ima potencijal da donese uštede od čak 45 milijardi dolara kroz povećanje operativne efikasnosti i smanjenje troškova održavanja starih infrastruktura.

Ključne komponente sporazuma uključuju:

- Obuku 100.000 državnih službenika do 2030. godine u područjima umjetničke inteligencije i novih tehnologija.
- Razvoj zajedničke platforme za cyber sigurnost, koja će omogućiti bolje praćenje i zaštitu podataka u realnom vremenu.
- Pokretanje 12-sedmičnog akceleratora za AI startupove, s ciljem podsticanja inovacija u javnom sektoru.
- Pružanje cloud kredita i stručne podrške za razvoj novih digitalnih usluga.

Ovaj sporazum predstavlja značajan korak prema digitalnoj transformaciji javnih usluga u Velikoj Britaniji, koji će im omogućiti da postanu agilniji, sigurniji i usmjereniji na korisnike (UK Government, 2025).

Ipak, prelazak u oblak otvara i važno pitanje upravljanja podacima i njihove bezbjednosti. Podaci državnih organa često sadrže lične informacije građana, klasifikovane podatke ili osjetljive finansijske evidencije. Zbog toga se prave razlike između **javnog oblaka**, koji dijeli infrastrukturu među različitim korisnicima, **privatnog oblaka** koji je rezervisan za jednu organizaciju i često se nalazi unutar nacionalnih data centara, te **hibridnog oblaka** koji kombinuje oba pristupa. Državne administracije često biraju hibridne modele – ključne baze podataka čuvaju u nacionalnim centrima, dok pomoćne aplikacije i sistemi za analitiku mogu biti hostovani kod komercijalnih provajdera. Time se postiže ravnoteža između sigurnosti, efikasnosti i inovativnosti.

Dodatno, treba imati u vidu i zakonske obaveze koje se tiču lokacije podataka. Mnoge zemlje propisuju da podaci građana moraju biti skladišteni unutar nacionalne teritorije ili da pristup takvim podacima može biti omogućen samo ovlašćenim institucijama. To znači da državne službe ne mogu nekontrolisano koristiti bilo koji cloud servis, već moraju provjeriti da li provajder obezbjeđuje usklađenost sa lokalnim propisima. U tom kontekstu se pojavljuju i nacionalne cloud platforme koje vode državne IT agencije ili centralni zavodi za informacione tehnologije.

Cloud takođe mijenja način na koji revizori pristupaju poslovanju organizacija. Umjesto klasične provjere server-soba, hardverske opreme i lokalnih backup kopija, revizori sada moraju da razumiju ugovorne odnose između institucije i provajdera, politike kontrole pristupa, načine šifrovanja podataka u oblaku, mehanizme vraćanja podataka nakon incidenta i evidenciju aktivnosti koja se vodi u cloud okruženju. Praćenje logova, analiza otisaka aktivnosti i procjena sigurnosnih sertifikata provajdera postaju sastavni dio revizorske metodologije u digitalnom dobu.

Internet stvari (Internet of Things – IoT)

Internet stvari predstavlja koncept u kojem različiti fizički objekti – uređaji, senzori, vozila, pametni mjerni sistemi, industrijske mašine ili čak uređaji u domaćinstvu – dobijaju mogućnost povezivanja na mrežu, razmjene podataka i automatizovanog reagovanja bez stalnog ljudskog učešća. Dok su tradicionalni informacioni sistemi podrazumijevali da čovjek unosi podatke i donosi odluke, IoT pomjera fokus ka sistemima koji sami prikupljaju informacije iz okruženja i mogu automatski pokrenuti određene procese (Buyya & Vahid Dastjerdi, 2016).

Suština IoT sistema je u tome da senzor otkriva promjenu u okolini (temperaturu, vlagu, kretanje, potrošnju energije, prisustvo vozila, nivo zagađenja vazduha, buku, vibracije i sl.), zatim taj podatak putem mreže šalje ka centralnom sistemu ili „gateway“ uređaju koji ga obrađuje, analizira

ili prosljeđuje dalje. Na osnovu analize, sistem može izvršiti automatsku radnju, kao što je uključivanje rasvjete, alarmiranje službe održavanja, blokiranje pristupa, automatsko otvaranje rampe ili čak pokretanje kompleksnijih procedura u državnim službama.

U javnoj upravi IoT nalazi sve širu primjenu. Pametni gradovi (smart cities) koriste senzore postavljene na javnoj infrastrukturi za upravljanje saobraćajem, optimizaciju javne rasvjete, praćenje kvaliteta vazduha i brže reagovanje komunalnih službi. Na primjer, pametna saobraćajna raskrsnica može da prilagodi trajanje zelenog svijetla u skladu sa stvarnim protokom vozila, čime se smanjuju gužve i emisija štetnih gasova. U zdravstvu, senzori mogu pratiti stanje pacijenata na daljinu i obavijestiti ljekara u slučaju pogoršanja. U vodovodnom sistemu IoT uređaji otkrivaju curenja u mreži i automatski upućuju dojavu nadležnom sektoru. Organi bezbjednosti mogu koristiti IoT kamere sa analitičkim modulima za prepoznavanje neuobičajenih obrazaca kretanja u javnim prostorima.

Specifičan primjer za državne organe je primjena IoT uređaja u sistemima granične kontrole, gdje senzori mogu registrovati ulazak vozila, prikupljati podatke o registarskim tablicama, prepoznavati oznake tereta i odmah obavijestiti carinske inspektore ili bezbjednosne službe o mogućim nepravilnostima. U poljoprivredi, koju država takođe nadgleda i subvencioniše, senzori se koriste za mjerenje vlažnosti zemljišta i optimizaciju navodnjavanja, što omogućava preciznu dodjelu subvencija i kontrolu njihovog namjenskog korišćenja.

Dubai je jedan od pionira u primjeni IoT tehnologije u urbanom razvoju (The Times of India, 2025). Grad implementira pametne sisteme za upravljanje saobraćajem, energijom i javnim uslugama, uključujući pametnu rasvjetu, pametne parkinge i sisteme za upravljanje vodom. Ovi sistemi omogućavaju real-time praćenje i optimizaciju resursa, čime se poboljšava efikasnost i smanjuju troškovi (Digi International, 2025). Holandija koristi IoT tehnologiju za unapređenje poljoprivredne proizvodnje i održivosti (Konica Minolta, 2020). Senzori se koriste za praćenje uslova u poljima, uključujući vlagu, temperaturu i kvalitet tla, što omogućava precizno navodnjavanje i upotrebu pesticida. Ova tehnologija pomaže u smanjenju otpada i povećanju prinosa, čime se doprinosi održivom razvoju (Digi International, 2025). U indijskoj saveznoj državi Tamil Nadu, dionica nacionalne ceste NH-32 između Tambarama i Tindivanama postala je prva u toj državi koja je potpuno integrisana u IoT mrežu Nacionalne uprave za autoceste (NHAI). Kroz pilot projekat, na ovoj 90 km dugoj dionici postavljeni su GPS senzori na ulične svjetiljke, omogućavajući automatsko uključivanje i isključivanje na osnovu sunčevog svijetla, čime se smanjuje potrošnja energije. Takođe, sistem prati kretanje i vrijeme odgovora vozila Hitne pomoći, patrolnih vozila i dizalica za uklanjanje, koristeći geo-ograničenja za osiguranje pridržavanja zona i operativne odgovornosti (The Times of India, 2025). Takođe, u Nagpuru je razvijen napredni sistem za sigurno upravljanje osjetljivim materijalima poput policijskih dokaza, ispitnih papira i povjerljivih dokumenata. Sistem koristi IoT tehnologiju za praćenje u stvarnom vremenu, detekciju anomalija putem senzora i aplikacijsku verifikaciju, čime se osigurava nepromjenljivost i sigurnost prenosa ovih materijala (The Times of India, 2025).

Ipak, kao i kod drugih tehnologija, prisutni su i rizici. IoT uređaji često imaju ograničene kapacitete za zaštitu jer su mali, jeftini i dizajnirani za masovnu primjenu, pa ponekad ne posjeduju dovoljno snažne mehanizme enkripcije. Ako takav uređaj bude kompromitovan, napadač može preko njega dobiti pristup širem informacionom sistemu, izazvati greške u automatizovanom odlučivanju ili čak manipulisati podacima u realnom vremenu. Zbog toga revizori moraju razumjeti kako se IoT

uređaji registruju u sistemu, ko upravlja njihovim pristupnim pravima, da li se čuvaju evidencije aktivnosti i kako se vrši nadzor nad komunikacijom između IoT uređaja i centralnih sistema.

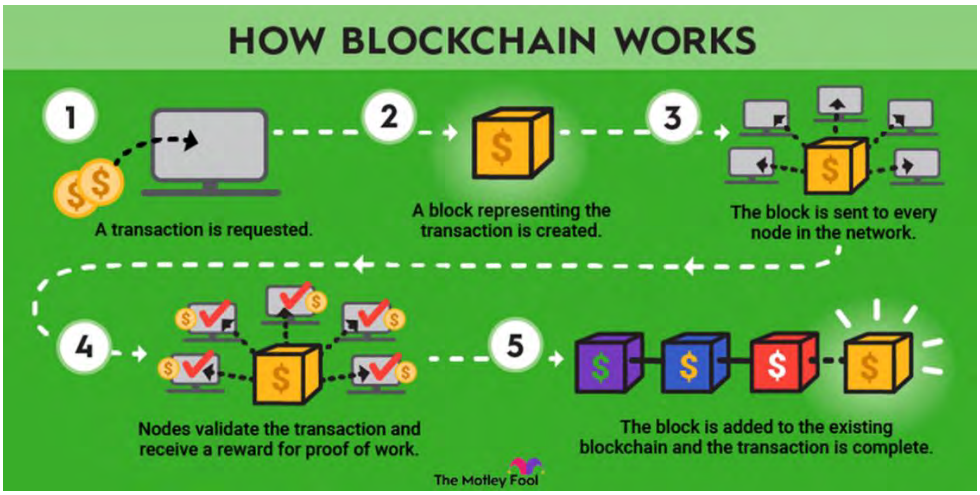
Pored toga, značajno pitanje je i upravljanje velikim količinama podataka koje IoT generiše. Ako hiljade senzora šalju podatke svakih nekoliko sekundi, sistem mora biti u stanju da ih skladišti, procesira i vizualizuje, a institucija mora imati definisane politike čuvanja, analize i brisanja podataka, posebno ako se prikupljaju podaci o građanima ili javnim površinama. Kombinacija IoT tehnologije sa vještačkom inteligencijom i obradom velikih podataka omogućava donošenje prediktivnih odluka – na primjer, automatsko predviđanje kada će neki dio infrastrukture otkazati i preventivno slanje tima za održavanje.

Blockchain

Blockchain je tehnologija koja omogućava sigurno i decentralizovano čuvanje podataka, bez potrebe da postoji centralna institucija koja kontroliše informacije. Podaci se čuvaju u „blokovima“ koji su hronološki povezani i kriptografski zaštićeni, što znači da jednom zabilježena informacija ne može biti promijenjena bez tragova koji bi odmah bili vidljivi svima u mreži. Svaki blok sadrži kriptografski sažetak prethodnog bloka (hash), vremensku oznaku i podatke transakcija, čime se stvara lanac blokova – blockchain – koji je transparentan, otporan na manipulaciju i lako provjerljiv.

Ova tehnologija je postala poznata kroz kriptovalute, naročito Bitcoin, koji je 2009. godine prvi primijenio blockchain za vođenje decentralizovanih digitalnih transakcija (Narayanan et al., 2016). Ideja je bila kreirati sistem u kojem učesnici mogu razmjenjivati vrijednost bez centralne banke, koristeći distribuciju podataka i kriptografske metode za verifikaciju i zaštitu. Blockchain je od tada evoluirao i primjenjuje se u mnogim drugim oblastima osim finansija.

Jedan od ključnih mehanizama sigurnosti blockchaina je heširanje – proces kojim se podaci pretvaraju u jedinstveni digitalni otisak (hash) koji predstavlja sadržaj bloka. Ako bilo koja informacija u bloku bude promijenjena, hash se mijenja, što automatski razotkriva neovlašćenu promjenu. Osim heširanja, blockchain koristi i digitalne potpise i konsenzusne protokole, poput Proof-of-Work ili Proof-of-Stake, koji omogućavaju da svi učesnici mreže potvrde tačnost podataka prije nego što se novi blok doda u lanac. Slika 12 prikazuje kako blockchain funkcioniše (The Motley Fool, 2025).



Slika 12. Princip funkcionisanja blokchain tehnologije

Za državne organe blockchain nudi značajne mogućnosti u transparentnom i sigurnom vođenju evidencija. Primjeri primjene uključuju elektronsko vođenje zemljišnih knjiga, registraciju javnih ugovora, upravljanje identitetima građana, nadzor lanaca nabavke i digitalno arhiviranje službenih dokumenata. Na primjer, kada se koristi blockchain za zemljišne registre, svaka transakcija, poput kupovine ili prenosa vlasništva, postaje trajno zabilježena i javno provjerljiva, što smanjuje mogućnost korupcije i prevara. U zdravstvu i socijalnim službama blockchain može pomoći u praćenju lanca vakcinacije ili distribucije socijalnih pomoći, osiguravajući da podaci budu autentični i nepromjenljivi.

Konkretno, Estonija je pionir u primeni blockchain tehnologije u javnoj upravi. Korišćenjem blockchaina Estonija osigurava integritet državnih podataka i omogućava građanima siguran i jednostavan pristup javnim uslugama. Ovaj pristup povećava povjerenje građana u institucije i smanjuje mogućnost manipulacije podacima (Turner Lee and Wnag, 2025). Takođe, indijska savezna država Kerala implementirala je blockchain tehnologiju u upravljanju zemljišnim knjigama kako bi eliminisala zemljišne sporove do 2031. godine. Ovaj sistem koristi blockchain za sprečavanje neovlašćenih promjena i falsifikovanja dokumenata, omogućavajući transparentnu i sigurnu provjeru vlasništva u realnom vremenu (The Times of India, 2025). Kina je razvila nacionalni sistem decentralizovanih identifikatora (China RealDID) koji koristi blockchain tehnologiju za verifikaciju identiteta građana. Ovaj sistem omogućava siguran pristup onlajn uslugama uz očuvanje privatnosti korisnika, u skladu sa zakonodavstvom koje zahtijeva upotrebu stvarnih identifikacija za onlajn naloge (Business Insider, 2023).

Blockchain je takođe osnova razvoja Web 3.0, koncepta interneta u kojem korisnici imaju veću kontrolu nad svojim podacima i digitalnim identitetom, dok decentralizovane aplikacije (DApps) omogućavaju nove oblike interakcije sa digitalnim servisima. Za državne organe Web 3.0 i blockchain mogu poboljšati sigurnost i transparentnost interakcije sa građanima, ali donose i izazove u smislu upravljanja identitetima, privatnosti podataka i interoperabilnosti sistema.

Međutim, blockchain nije bez svojih izazova. Skalabilnost, energetska potrošnja (posebno kod Proof-of-Work sistema), regulatorna pitanja i privatnost podataka ostaju ključni problemi. Za revizore, razumijevanje kako blockchain funkcioniše, koji podaci se čuvaju, kako se upravlja

pristupom i ko ima ovlašćenja za potvrdu transakcija, ključno je za procjenu rizika i osiguranje integriteta digitalnih procesa.

Da zaključimo, moderne tehnološke platforme o kojima je bilo riječi omogućavaju organizacijama da efikasnije obrađuju informacije, donose bolje odluke i unaprijede kvalitet usluga koje pružaju građanima. Vještačka inteligencija, sa svojim različitim oblicima – od mašinskog učenja i neuronskih mreža do ekspertnih sistema i generativne AI – omogućava državnim organima da analiziraju velike količine podataka i automatizuju zadatke koji su ranije zahtijevali značajan ljudski angažman. Primjena ovih tehnologija u javnom sektoru uključuje optimizaciju resursa, poboljšanje procesa donošenja odluka i podršku u upravljanju rizicima.

Veliki podaci, kao osnov za AI aplikacije, pružaju mogućnost praćenja i analiziranja informacija u realnom vremenu. Međutim, njihove karakteristike – obim, brzina, raznolikost i pouzdanost – donose i izazove, posebno u pogledu zaštite privatnosti građana i sigurnosti podataka.

Računarstvo u oblaku omogućava državnim institucijama fleksibilno korišćenje infrastrukturnih i softverskih resursa, smanjujući troškove i povećavajući skalabilnost. Ipak, upravljanje pristupom, zaštita podataka i odabir odgovarajućih provajdera postaju ključni zadaci u održavanju sigurnosti i kontinuiteta rada.

Internet stvari omogućava prikupljanje podataka iz fizičkog svijeta putem senzora i pametnih uređaja. U državnom sektoru to se koristi za pametne gradove, upravljanje saobraćajem, energijom, vodovodom i održavanje infrastrukture. Na ovaj način organi mogu donositi brže i informisanije odluke, smanjiti troškove i unaprijediti sigurnost i kvalitet usluga.

Blockchain tehnologija, sa svojom sposobnošću da distribuirano i nepromjenljivo čuva podatke, pruža osnovu za transparentne i sigurne evidencije, uključujući registarske i finansijske podatke, i otvara put za razvoj Web 3 servisa u javnom sektoru.

Tabela 5 sumira moderne tehnološke platforme, njihove primjene u državnim organima, kao i njihove prednosti i rizike.

Tabela 5. Moderne tehnološke platforme

Tehnološka platforma	**Primjena u državnim organima**	**Prednosti**	**Rizici / izazovi**
Vještačka inteligencija (AI)	Analiza velikih podataka, automatizacija procesa, podrška u donošenju odluka, generativna AI za komunikacije i izradu izvještaja	Brže donošenje odluka, smanjenje ljudske greške, povećanje efikasnosti, optimizacija resursa	Privatnost podataka, algoritamska pristrasnost, greške u modelima, sigurnost podataka
Veliki podaci (Big Data)	Praćenje trendova, statističke analize, planiranje javnih politika, predikcija potreba građana	Uvid u velike količine informacija, podrška za AI, optimizacija resursa	Privatnost, zaštita podataka, kvalitet i pouzdanost podataka, složenost analize

Računarstvo u oblaku (Cloud)	Centralizacija IT resursa, pružanje softverskih usluga, backup i disaster recovery, kolaboracija među organima	Fleksibilnost, smanjenje troškova infrastrukture, skalabilnost, pristup s različitih lokacija	Sigurnost podataka, kontrola pristupa, zavisnost o provajderu, regulativa o podacima
Internet stvari (IoT)	Pametni gradovi (saobraćaj, energija, voda), nadzor infrastrukture, upravljanje javnim uslugama	Real-time praćenje, efikasno upravljanje resursima, smanjenje troškova, bolja usluga građanima	Sigurnost uređaja i mreže, privatnost građana, interoperabilnost uređaja, održavanje senzora
Blockchain	Evidencija registara, finansijske transakcije, digitalni identitet, transparentnost javnih procesa	Sigurnost i nepromjenljivost podataka, transparentnost, decentralizacija, smanjenje prevara	Skalabilnost, energetska potrošnja, kompleksnost implementacije, regulativa

Za revizore, razumijevanje ovih tehnologija postaje sve važnije. Oni moraju biti u stanju da procijene rizike povezane sa privatnošću, sigurnošću i integritetom podataka, kao i da pruže smjernice za primjenu kontrola i procedura koje osiguravaju zakonit i efikasan rad državnih organa. Integracija ovih tehnologija mijenja način na koji revizori planiraju i izvode svoje zadatke, zahtijevajući od njih kontinuirano praćenje inovacija i razumijevanje tehničkih i organizacionih implikacija.

Na kraju, moderne tehnološke platofrme pružaju državnim institucijama neuporedivu moć u obradi informacija i upravljanju procesima, ali istovremeno nameću i visoke standarde bezbjednosti, transparentnosti i odgovornosti. Uloga revizora je da pomogne organima da ove tehnologije koriste odgovorno, efikasno i u skladu sa zakonskim i etičkim normama, osiguravajući da koristi koje donose moderni sistemi budu maksimalno iskorišćene, a rizici minimalizovani.

2. Baze podataka

U savremenom revizorskom okruženju, poznavanje različitih tehnologija za pohranu i obradu podataka postaje ključna vještina. Dok relacioni model pruža temelj za organizaciju podataka u strukturisanim tabelama, Big Data i Cloud Computing omogućavaju rad sa ogromnim količinama podataka i pristup informacijama preko interneta. Razumijevanje osnovnih principa ovih tehnologija pomaže revizoru da identifikuje potencijalne rizike, nepravilnosti i propuste u sistemima, ali i da bolje procijeni integritet, dostupnost i sigurnost podataka.

2.1. Relacioni model

Relacioni model je najrasprostranjeniji način organizacije podataka u savremenim informacionim sistemima. Većina baza podataka koje koriste državni organi, javne institucije ili računovodstveni softveri zasniva se upravo na ovom modelu. Zbog toga je važno da revizor, čak i ako nije informatičar, razumije osnovne principe po kojima se podaci organizuju, jer će upravo u tim strukturama tražiti tragove nepravilnosti, nelogičnosti i potencijalnih manipulacija.

Već smo rekli da je baza podataka integrisani skup međusobno povezanih datoteka u kojima su smješteni slogovi ili zapisi sa odgovarajućom strukturom polja. Modeli podataka nam omogućavaju konceptualni pogled na bazu podataka, koji je jasniji za korisnika. Relacioni model predstavlja bazu podataka u vidu skupa tabela u kojima se čuvaju podaci. Svaka tabela predstavlja određeni entitet, na primjer:

- Zaposleni
- Odsjeci
- Korisnici sistema
- Računi
- Transakcije.

Redovi u tabeli nazivaju se zapisi ili slogovi, a kolone atributi. Svaki slog predstavlja jedan konkretan primjer entiteta – jedan zaposleni, jedan odsjek, jedna transakcija.

Da bi se svaki slog mogao jednoznačno identifikovati, koristi se **primarni ključ (PK)**. To je kolona (ili kombinacija kolona) čija se vrijednost ne smije ponavljati i ne smije biti prazna. Primjeri primarnih ključeva su: JMBG, ID korisnika, broj transakcije.

Ako revizor pregledom baze primijeti da tabela ima slogove bez ključnih podataka (npr. zaposleni bez matičnog broja ili odsjeka), to može ukazivati na neuredno vođenje evidencije ili pokušaj manipulacije sistemom. Postojanje duplih primarnih ključeva ili slogova bez ključa može značiti da je došlo do ručnog unosa mimo sistema ili pokušaja skrivanja tragova o stvarnoj transakciji.

Između tabela mogu postojati tri vrste odnosa (veza) koje su prikazane u Tabeli 6 (Kašćelan, 2016).

Tabela 6. Vrste odnosa u relacionom modelu

Vrsta odnosa	Objašnjenje	Revizorski značaj
Jedan prema jedan (1:1)	Svakom zapisu iz prve tabele odgovara tačno jedan zapis iz druge.	Rijetko se koristi. Ako se pojavi duplikat, može značiti duplo knjiženje.
Jedan prema više (1:N)	Jedan odsjek ima više zaposlenih.	Jedan od najčešćih odnosa. Revizor provjerava da li svi zaposleni pripadaju važećim odsjecima.
Više prema više (M:N)	Jedan zaposleni može biti na više projekata i obrnuto.	Implementira se trećom tabelom. Revizor treba provjeriti da li postoji evidencija za oba pravca veze.

Kada želimo povezati dvije tabele u odnosu **1 prema N**, u tabelu koja predstavlja N (više zapisa) dodaje se **spoljnji ključ (SK)**, što znači da se u tu tabelu unosi kolona koja sadrži vrijednosti primarnog ključa iz glavne (nadređene) tabele. Na primjer, jedan odsjek može imati više zaposlenih, pa se u tabeli Zaposleni dodaje kolona ID_ODSJEKA koja se odnosi na primarni ključ u tabeli Odsjeci. Sistemske kontrole ne dozvoljavaju da se unese vrijednost spoljnjeg ključa koja ne postoji u glavnoj tabeli (to se zove **referencijalni integritet** podataka). Dakle, ne može se dodati zaposleni kojem je ID_ODSJEKA = 999 ako u tabeli Odsjeci takav odsjek ne postoji.

Kod odnosa **N prema M**, direktno povezivanje nije moguće jer bi došlo do dupliranja podataka. Zato se uvodi posebna **povezna tabela**, koja sadrži dva spoljnja ključa – jedan koji pokazuje na prvu tabelu, a drugi na drugu. Tako se, na primjer, za praćenje ko radi na kojem projektu uvodi povezna tabela Zaposleni_Projekti koja sadrži dva spoljnja ključa ID_ZAPOSLENOG i ID_PROJEKTA. Na taj način sistem jasno pokazuje da jedan zaposleni može biti dodijeljen na više projekata, i da jedan projekat može imati više zaposlenih, a sve to bez ponavljanja podataka. Za spoljnje ključeve povezne tabele takođe postoje kontrole sistema koje čuvaju referencijalni integritet podataka (Kašćelan, 2016).

Revizor u informacionim sistemima ne traži samo dokumente – on traži neusklađenosti u podacima. Poznavanje relacionog modela omogućava mu da postavi pitanja poput:

- Postoje li zapisi bez pripadajuće veze?
- Ima li više zapisa sa istim ključem?
- Da li su veze između tabela logične i potpune?

U praksi, neusklađeni odnosi između tabela često otkrivaju neprijavljene promjene, neregistrovane korisnike, fiktivne radnike ili lažne naloge.

Na primjer, pretpostavimo da u bazi podataka tabele Odsjeci i Zaposleni izgledaju ovako:

ID_ODSJEKA (PK)	Naziv odsjeka
101	Finansije
102	Ljudski resursi

103	IT služba

ID_ZAPOSLENOG (PK)	Ime i prezime	JMBG	ID_ODSJEKA (SK)
2001	Marko Jovanović	1203996770021	101
2002	Jelena Petrović	1506988770022	103
2003	Ivan Marković		999

Revizor može uočiti da ID_ODSJEKA 999 ne postoji – „viseći“ zapis, što je indikator da je odsjek možda obrisan ili je zapis ručno izmijenjen mimo kontrola sistema. Takođe, s obzirom da nedostaje JMBG revizor može postaviti pitanje da li je zaposleni stvarno postojao ili je unos fiktivan.

Pretpostavimo da u bazi postoji i tabela Projekti:

ID_PROJEKTA (PK)	Naziv projekta
P001	Digitalizacija arhive
P002	Modernizacija ERP-a

Ako jedan zaposleni može raditi na više projekata, a jedan projekat ima više zaposlenih, uvodi se povezna tabela Zaposleni_Projekti:

ID_ZAPOSLENOG (SK)	ID_PROJEKTA (SK)
2001	P001
2001	P002
2002	P001
2007	P001

Ako postoji projekat u tabeli Projekti, ali nema nijednog zaposlenog povezanog u tabeli Zaposleni_Projekti, to može značiti da se vodi projekat bez stvarnog angažmana – potencijalni indikator fiktivnog projekta ili planiranja troškova koji se ne realizuju. Postojanje zaposlenog 2007 u Zaposleni_Projekti, kojeg nema u tabeli Zaposleni, može značiti da je taj zaposleni fiktivan i unešen ručno mimo kontrola sistema, kako bi se mogle realizovati fiktivne isplate u okviru projekta P001.

Iz revizorskog ugla, pravilno definisani odnosi u bazi podataka ukazuju na postojanje kontrolisanog i dosljednog sistema upravljanja podacima. Revizor provjerava da li spoljnji ključevi zaista vode ka postojećim primarnim ključevima, što je osnov referencijalnog integriteta. Posebnu pažnju obraća na postojanje „izolovanih zapisa“, npr. zaposlenih kojima nije dodijeljen nijedan odsjek ili projekata kojima nije pridružen nijedan zaposleni, jer takvi slučajevi mogu ukazivati na nepotpune ili ručno unesene podatke mimo standardnih procedura. Revizor takođe

analizira da li su primarni ključevi jedinstveni i automatski generisani, kako bi se spriječilo dupliranje evidencije ili naknadne manipulacije podacima.

U savremenim informacionim sistemima svaka baza podataka ima mogućnost vođenja takozvanih **logova promjena (audit logs)**, gdje se bilježi ko je, kada i koji zapis izmijenio ili obrisao. Iako revizor ne mora poznavati tehničku strukturu logova, treba da bude svjestan njihovog značaja kao digitalnog traga koji može potvrditi ili osporiti autentičnost unosa u bazi podataka. Na primjer, ako se u tabeli Zaposleni pojavi zapis bez JMBG-a ili sa nepostojećim ID_ODSJEKA, log može otkriti tačan korisnički nalog i vrijeme kada je ta izmjena izvršena, što pomaže u utvrđivanju odgovornosti i otkrivanju eventualnih manipulacija. Revizor treba da zatraži uvid ili izvještaj iz logova sistema kada postoji sumnja da je došlo do ručne intervencije mimo standardnih procedura unosa, jer pravilno vođenje logova predstavlja ključni element interne kontrole i integriteta baze podataka.

U relacionim bazama je moguće definisati **korisnička ovlašćenja**. Svakom korisniku ili korisničkoj grupi dodjeljuje se određeni nivo pristupa: samo čitanje (read-only), unos novih podataka, izmjena postojećih zapisa ili brisanje. U dobro kontrolisanom sistemu revizor može tražiti izvod iz baze u kojem se jasno vidi ko ima pravo da mijenja ključne tabele, poput one koja sadrži evidenciju zaposlenih, korisničke naloge ili projektnu dokumentaciju. Ako korisnik koji nije zadužen za određeni proces ima pravo da mijenja te podatke, to predstavlja indikator mogućnosti zloupotrebe. Revizor treba da provjeri postoji li tabela ili sistemska evidencija korisničkih prava (npr. **USERS, ROLES, PRIVILEGES**) i da li se ista poklapa sa organigramom institucije i opisima radnih zadataka. Na taj način se potvrđuje da su podaci ne samo tehnički ispravni, već i zaštićeni od neovlašćenih intervencija.

2.2. Big data

Pojam Big Data odnosi se na obradu i analizu veoma velikih, kompleksnih i raznovrsnih skupova podataka koje tradicionalni sistemi baza podataka ne mogu efikasno obraditi. Big Data karakterišu tri ključna svojstva, poznata i kao 3V:

- Volume (Obim): ogromna količina podataka koja stalno raste – od milijardi transakcija i korisničkih aktivnosti do senzorskih podataka i IoT uređaja.
- Velocity (Brzina): podaci se generišu i prenose gotovo u realnom vremenu, što zahtijeva brze i kontinuirane procese obrade.
- Variety (Raznovrsnost): podaci dolaze u različitim oblicima – strukturirani (tabele), polustrukturirani (JSON, XML) i nestrukturirani (e-mailovi, dokumenti, video i audio-zapisi).

Za revizore, Big Data predstavlja novu priliku, ali i izazov. S jedne strane, alati za analizu velikih podataka omogućavaju automatsko prepoznavanje obrazaca, nepravilnosti i potencijalnih rizika u ogromnim skupovima transakcija, što značajno poboljšava efikasnost revizije. S druge strane, revizor mora razumjeti da veliki obim podataka zahtijeva posebne procedure za provjeru tačnosti i integriteta, jer se ne mogu svi zapisi pregledati ručno.

Big Data sistemi često koriste tehnologije poput Hadoop-a ili Spark-a, koje omogućavaju distribuiranu obradu podataka preko više računara. Tako se čak i ogromne baze podataka mogu analizirati paralelno i brzo. Za revizore je ključno znati da ne moraju poznavati sve tehničke detalje, već da razumiju osnovne principe:

- podaci dolaze iz različitih izvora (ERP sistemi, IoT uređaji, društvene mreže),
- sistem koristi automatizovane algoritme za agregaciju i obradu,
- kontrola kvaliteta i integritet podataka su ključni za pouzdane rezultate analize.

Kada revizor radi s Big Data, važno je da provjeri:

- Da li su izvori podataka validni i pouzdani.
- Da li postoje kontrole za čišćenje i filtriranje podataka (data cleaning).
- Da li analitički alati prate integritet podataka i loguju promjene.
- Da li je pristup podacima zaštićen i dodijeljena su prava pristupa u skladu s internim kontrolama.

Na taj način, Big Data postaje moćan alat za reviziju, omogućavajući identifikaciju nepravilnosti koje bi u tradicionalnoj bazi podataka bile teško otkrivene.

2.3. Cloud computing

Cloud computing (računarstvo u oblaku) predstavlja način pružanja računarskih resursa – poput servera, skladišta podataka, softverskih aplikacija i mrežnih usluga – preko interneta. Umjesto da organizacija kupuje i održava vlastite servere i softver, koristi se infrastruktura i aplikacije koje se nalaze na udaljenim serverima, kojima se pristupa putem interneta.

Za revizore, cloud computing donosi novu dimenziju kontrole i rizika. Kada se podaci i aplikacije nalaze u oblaku, revizor mora provjeriti:

- Prava pristupa i vlasništvo nad podacima: ko može pristupiti sistemu i podacima, i da li su pristupna prava pravilno definisana.
- Sigurnost i enkripcija podataka: da li su podaci zaštićeni pri prenosu i skladištenju, te da li se koristi HTTPS, VPN ili druga zaštita.
- Kontrole integriteta podataka: da li postoje logovi aktivnosti, automatske provjere i audit trail koji omogućavaju praćenje promjena.
- Uslovi ugovora s provajderom oblaka: da li postoje garancije za sigurnost, privatnost podataka i dostupnost usluga.
- Kontinuitet poslovanja i backup: da li provajder nudi opcije za oporavak podataka u slučaju kvara ili incidenta.

Cloud computing omogućava organizacijama da pristupaju naprednim tehnologijama i analizama (uključujući Big Data i AI) bez potrebe za velikim internim resursima. Međutim, revizor mora razumjeti da fizička lokacija podataka, odgovornosti provajdera i interne kontrole organizacije direktno utiču na pouzdanost informacija koje se koriste za reviziju.

Kroz cloud revizor može provjeriti sigurnost, tačnost i dostupnost podataka, ali i identifikovati potencijalne rizike povezane s pristupom, kontrolom i integritetom podataka u digitalnom okruženju.

Tabela 7 objedinjuje sve 3 tehnologije o kojima smo govorili u ovom poglavlju kao i revizorski fokus u vezi njih.

Tabela 7. Tehnologije za baze podataka i ključne kontrole

Tehnologija	Osnovna ideja	Primjeri u praksi	Revizorski fokus
Relacioni model	Podaci se čuvaju u tabelama; veze se ostvaruju primarnim i stranim ključevima	Tabele Zaposleni, Odsjeci, Projekti; veze 1:N i M:N	Provjera integriteta podataka, jedinstvenosti primarnih ključeva, validnosti stranih ključeva, „viseći“ zapisi, logovi aktivnosti
Big Data	Analiza i obrada vrlo velikih i raznovrsnih skupova podataka koji se brzo generišu	ERP sistemi, transakcioni podaci, IoT senzori, društvene mreže	Identifikacija nepravilnosti, anomalija i obrazaca, kontinualna revizija, sigurnost pristupa podacima, integritet i tačnost podataka
Cloud Computing	Pristup resursima, podacima i aplikacijama preko interneta bez lokalnog servera	SaaS (npr. Google Workspace), IaaS (AWS), PaaS (Azure)	Prava pristupa i vlasništvo nad podacima, enkripcija, audit trail, backup i kontinuitet poslovanja, sigurnost i dostupnost podataka

Sve tri tehnologije – relacioni model, Big Data i Cloud Computing – predstavljaju različite pristupe upravljanju podacima, a razumijevanje njihovih principa i kontrola pomaže revizoru da efikasno prati integritet, dostupnost i sigurnost informacija u digitalnom okruženju.

3. Elektronski sistemi za upravljanje dokumentima (eDMS)

Elektronski sistemi za upravljanje dokumentima (eDMS – electronic Document Management Systems) predstavljaju ključnu komponentu digitalne transformacije organizacija, koja objezbjeđuje efikasno upravljanje, pohranjivanje i pristup dokumentima u elektronskom formatu (AIIM, 2021). Ovi sistemi omogućavaju organizacijama da pređu sa tradicionalnog papira na digitalno poslovanje, čime se povećava efikasnost, smanjuju troškovi i poboljšava usklađenost sa zakonodavstvom (Laudon & Laudon, 2021).

Prema definiciji eDMS je softverski sistem koji omogućava organizacijama da kreiraju, pohranjuju, upravljaju i prate elektronske dokumente kroz njihov životni ciklus. To uključuje procese kao što su skeniranje, indeksiranje, arhiviranje, pretraga, distribucija i uništavanje dokumenata u skladu sa zakonskim propisima i internim politikama organizacije (ISO 15489-1, 2016).

Ključne komponente eDMS-a

eDMS obuhvata nekoliko ključnih komponenti koje omogućavaju efikasno upravljanje dokumentima (AIIM, 2021; ISO 15489-1, 2016):

- Skladištenje dokumenata: Centralizovano pohranjivanje dokumenata u elektronskom formatu, omogućavajući lako pretraživanje i pristup.
- Indeksiranje i metapodaci: Dodavanje metapodataka (kao što su datum, autor, kategorija) dokumentima radi lakše pretrage i organizacije.
- Verzionisanje: Praćenje i upravljanje različitim verzijama dokumenata, omogućavajući povratak na prethodne verzije po potrebi.
- Kontrola pristupa: Definisanje prava pristupa korisnicima i grupama, osiguravajući da samo ovlašćeni korisnici mogu pristupiti određenim dokumentima.
- Radni tokovi (workflow): Automatizacija procesa odobravanja, revizije i distribucije dokumenata, čime se smanjuje potreba za manuelnim intervencijama i ubrzava poslovanje.
- Arhiviranje i uništavanje: Dugoročno čuvanje dokumenata u skladu sa zakonskim zahtjevima i internim politikama, kao i bezbjedno uništavanje dokumenata koji više nijesu potrebni.

Prednosti implementacije eDMS-a

Implementacija eDMS-a donosi brojne prednosti organizacijama (AIIM, 2021; Laudon & Laudon, 2021):

- Povećana efikasnost: Brži pristup dokumentima smanjuje vrijeme potrebno za pronalaženje informacija i donošenje odluka.
- Smanjenje troškova: Eliminacija potrebe za fizičkim skladištenjem papira smanjuje troškove prostora, papira i štampe.
- Poboljšana sigurnost: Kontrola pristupa i praćenje aktivnosti korisnika povećavaju sigurnost podataka i smanjuju rizik od neovlašćenog pristupa.
- Usklađenost sa zakonodavstvom: Automatsko praćenje i primjena zakonskih rokova za čuvanje i uništavanje dokumenata pomaže organizacijama da ostanu u skladu sa propisima.

- Bolja saradnja: Omogućavanje zajedničkog rada na dokumentima u realnom vremenu poboljšava timsku saradnju i produktivnost.

Aspekti eDMS-a važni za reviziju

Za revizore, eDMS sistemi predstavljaju posebno važnu komponentu digitalne infrastrukture, jer direktno utiču na tačnost, sigurnost i usklađenost sa zakonodavstvom u upravljanju dokumentima. Prilikom revizije sljedeći aspekti su ključni (ISACA, 2021):

- Praćenje i audit trail: eDMS sistemi omogućavaju evidentiranje svih aktivnosti vezanih za dokumente. Svaka akcija, kao što je kreiranje, izmjena, pregled ili brisanje dokumenta, može biti zabilježena vremenskim pečatom i identitetom korisnika. Ovaj audit trail je ključan za identifikaciju potencijalnih nepravilnosti i osiguranje odgovornosti. Na primjer, revizor može provjeriti da li je dokument odobren od strane ovlašćenog lica prije nego što je postao zvaničan.
- Kontrola pristupa i sigurnost: Definisanje i implementacija politika pristupa korisnicima i grupama osigurava da samo ovlašćeni korisnici mogu pristupiti određenim dokumentima. Revizori procjenjuju da li su ove kontrole efikasne, kako je implementirana autentikacija i da li pristup dokumentima odgovara internim pravilima i zakonskim zahtjevima.
- Usklađenost sa zakonodavstvom: eDMS treba biti konfigurisan tako da automatski primjenjuje zakonske rokove za čuvanje i uništavanje dokumenata. Revizor provjerava da li organizacija pravilno upravlja dokumentima u skladu sa relevantnim zakonima i internim procedurama. Ovo uključuje provjeru arhiviranja, sigurnog uništavanja i evidentiranja svih aktivnosti (ISO 15489-1, 2016).
- Integracija sa drugim sistemima: Elektronski dokumenti često se koriste u kombinaciji sa ERP, CRM ili drugim poslovnim sistemima. Revizori trebaju provjeriti da li su ove integracije pravilno implementirane, da li podaci teku sigurno i tačno između sistema i da li je održan integritet podataka (Laudon & Laudon, 2021).
- Obuka i svijest korisnika: Efikasno korišćenje eDMS-a zahtijeva odgovarajuću obuku korisnika. Revizor procjenjuje da li je obuka adekvatna, da li korisnici razumiju svoje odgovornosti u vezi sa sigurnošću podataka i pravilnim korišćenjem sistema, te da li se procedure i pravila poštuju u praksi (AIIM, 2021).

Ukratko, za revizore eDMS je više od softverskog alata – on je sredstvo za osiguranje da organizacija može pouzdano i efikasno upravljati dokumentima, smanjiti rizik od nepravilnosti i osigurati usklađenost sa zakonima. Procjena i testiranje svih navedenih aspekata pomažu revizorima da daju objektivne preporuke i povećaju pouzdanost informacionog sistema.

4. E-portal

E-portal je važna komponenta javne uprave, jer omogućava građanima, preduzećima i drugim korisnicima pristup elektronskim uslugama i informacijama putem interneta. Za državne organe, implementacija e-portala nije samo tehnološki izazov, već i prilika za unapređenje transparentnosti, efikasnosti i odgovornosti u radu. Međutim, kako bi se osigurala pravilna implementacija i funkcionisanje e-portala, veoma je važna uloga revizije koja prati usklađenost sa zakonodavstvom, pravilnicima i internim procedurama.

U ovom poglavlju biće razmotren značaj e-portala za državne organe, izazovi u njihovoj implementaciji, koristi koje donose, kao i uloga revizije u obezbjeđivanju njihove efikasnosti i usklađenosti. Poseban akcenat biće stavljen na specifičnosti crnogorskog konteksta.

Trenutno stanje e-portala u Crnoj Gori

E-portali u Crnoj Gori predstavljaju osnovni kanal za pružanje elektronskih usluga građanima i privredi, u skladu sa nacionalnom strategijom digitalizacije javne uprave (Ministarstvo javne uprave, 2022). Kroz ove portale korisnici mogu pristupiti različitim administrativnim uslugama, kao što su podnošenje zahtjeva za lična dokumenta, plaćanje dažbina, prijava poreza i pristup informacijama o javnim procedurama. Implementacija e-portala u Crnoj Gori je počela u okviru EU projekata podrške digitalnoj transformaciji i uz primjenu međunarodnih standarda za elektronsko upravljanje (Open Government Partnership, 2022; European External Action Service, 2019).

Prema podacima crnogorske vlade njihov portal pruža preko 500 usluga u nadležnosti 50 institucija, od kojih je 155 elektronskih, a 349 su informacije o korišćenju različitih vladinih usluga. Najpopularnije usluge su dostavljanje podataka iz prekršajnih evidencija, prijave za polaganje stručnih ispita za rad u državnim organima i dostavljanje podataka iz krivičnih evidencija (Balkan Insight, n. d.).

Trenutni sistemi u praksi omogućavaju građanima jednostavan i brz pristup informacijama i uslugama, ali se javlja nekoliko izazova koji su važni za revizore. Prvo, interoperabilnost između različitih državnih baza podataka nije uvijek optimalna, što može dovesti do nepotpunih ili netačnih podataka koji se koriste u procesu odlučivanja. Drugi izazov je sigurnost podataka i kontrola pristupa, jer e-portali sadrže lične i povjerljive informacije građana i privrednih subjekata (ISO/IEC 27001, 2022). Treći izazov je praćenje korisničkih aktivnosti i audit trail, što je ključno za reviziju i identifikaciju eventualnih nepravilnosti u radu državnih organa.

Za državne revizore, koji procjenjuju funkcionalnost i pouzdanost e-portala, posebno je značajno da razumiju strukturu portala, integraciju sa drugim sistemima (npr. registri stanovništva, porezna administracija) i pravila zaštite podataka. Revizija e-portala nije ograničena samo na tehničku ispravnost, već obuhvata i procjenu zakonitosti, efikasnosti i transparentnosti pruženih usluga (ISACA, 2021).

Prednosti e-portala za građane i državne organe

E-portali značajno unapređuju dostupnost i kvalitet javnih usluga, pružajući građanima i privredi mogućnost da elektronski obavljaju administrativne procedure, bez potrebe za fizičkim dolaskom

u institucije. To povećava efikasnost, smanjuje vrijeme potrebno za obavljanje poslova i doprinosi transparentnosti rada državnih organa (UN DESA, 2024). Na primjer, putem e-portala građani mogu pratiti status svojih zahtjeva u realnom vremenu, dobiti obavještenja o rokovima i automatski generisati potvrde ili izvještaje potrebne za različite administrativne procese.

Za državne organe e-portali omogućavaju centralizaciju podataka i bolju koordinaciju između različitih odjeljenja. Digitalizacija procesa smanjuje rizik od grešaka koje nastaju kod manuelnog unosa podataka i olakšava praćenje izvršenja zadataka. Implementacija e-portala takođe omogućava bolju evidenciju i audit trail, što je od ključnog značaja za revizore. Svaka aktivnost korisnika – od pristupa dokumentima do promjena u zahtjevima – može biti zabilježena i analizirana, čime se povećava odgovornost službenika i smanjuje mogućnost zloupotrebe (ISO/IEC 27001, 2022).

Pored tehničkih i operativnih prednosti, e-portali doprinose i boljoj usklađenosti sa zakonodavstvom i regulativom. Automatizacija procesa osigurava da su zakonski rokovi i procedure ispoštovani, a revizori mogu lakše provjeriti da li organi javne uprave postupaju u skladu sa propisima (ISACA, 2021).

Međutim, e-portali nijesu samo tehničko rješenje – oni zahtijevaju i promjene u organizacionoj kulturi. Službenici moraju biti obučeni za rad sa digitalnim alatima, razumjeti svoje odgovornosti u zaštiti podataka i redovno pratiti sisteme kako bi se osigurala tačnost i ažurnost informacija (UN DESA, 2024).

Funkcionalnosti e-portala za korisnike i javnost

E-portali služe kao centralna tačka za interakciju građana, preduzeća i drugih korisnika sa državnim organima. Njihova glavna svrha je da pojednostave pristup informacijama, smanje potrebu za fizičkim posjetama i ubrzaju pružanje javnih usluga (UN DESA, 2024). Funkcionalnosti e-portala obuhvataju nekoliko ključnih aspekata:

1. Pristup informacijama

E-portali omogućavaju korisnicima da lako pronađu zakone, propise, procedure i druge relevantne dokumente. Pretraživanje se često vrši po kategorijama, ključnim riječima ili datumu objave. Ovaj pristup poboljšava transparentnost državnih organa i omogućava revizorima da provjere da li informacije koje su javno dostupne odgovaraju internim evidencijama i propisima (ISO 15489-1, 2016).

2. Elektronske usluge i prijave

Kroz e-portal građani i firme mogu podnositi različite zahtjeve, prijave, prijaviti promjene podataka ili izvršiti plaćanja. Primjeri uključuju registraciju vozila, podnošenje poreskih prijava, zahtjeve za izdavanje dozvola i drugih sertifikata. Revizori trebaju provjeriti da li sistem osigurava tačnost, integritet i bezbjednost podataka tokom ovih procesa, kao i da li postoji adekvatan audit trail (ISACA, 2021).

3. Personalizacija i autentikacija korisnika

Savremeni e-portali omogućavaju korisnicima da kreiraju naloge i personalizuju svoje interakcije. Autentikacija se vrši putem različitih metoda, uključujući korisničke lozinke, dvofaktorsku

autentikaciju i digitalne sertifikate. Za revizore je važno procijeniti sigurnost ovih metoda, zaštitu ličnih podataka i efikasnost kontrole pristupa (ISO/IEC 27001, 2022).

4. Obavještavanje i praćenje statusa zahtjeva

E-portali omogućavaju korisnicima da prate status svojih zahtjeva u realnom vremenu i da dobijaju automatska obavještenja o promjenama. Ovo smanjuje potrebu za dodatnom komunikacijom sa službenicima i povećava efikasnost. Revizori mogu koristiti ove podatke kako bi procijenili koliko efikasno i pravovremeno organi obavljaju svoje funkcije (UN DESA, 2024).

5. Interaktivna komunikacija i povratne informacije

Mnogi e-portali nude mogućnost slanja povratnih informacija, pritužbi ili sugestija, kao i direktnu komunikaciju sa nadležnim službama. Ove funkcionalnosti omogućavaju građanima da aktivno učestvuju u poboljšanju javnih usluga, a revizorima daju uvid u kvalitet procesa i korisničko zadovoljstvo.

6. Pristup podacima u skladu sa zakonodavstvom o zaštiti podataka

E-portali moraju biti u skladu sa nacionalnim i međunarodnim zakonodavstvom o zaštiti ličnih podataka, uključujući GDPR (General Data Protection Regulation) (European Commission, 2016) i lokalne zakone (Zakon o zaštiti podataka o ličnosti, 2024). Revizori trebaju provjeriti da li portal osigurava privatnost podataka, enkripciju komunikacije i kontrolu pristupa kako bi se spriječila neovlašćena upotreba ili curenje informacija (ISO/IEC 27001, 2022; UN DESA, 2024).

Sve ove funkcionalnosti zajedno čine e-portal moćnim alatom za modernu upravu, omogućavajući brže, transparentnije i efikasnije pružanje javnih usluga, dok istovremeno pružaju revizorima jasan uvid u procese i kontrolu rizika.

Integracija e-portala sa drugim sistemima i podacima

E-portali u državnoj administraciji rijetko funkcionišu izolovano. Oni su obično povezani sa drugim informacionim sistemima, kao što su sistemi za upravljanje dokumentima (eDMS), baze podataka državnih registara, ERP sistemi, sistemi za plaćanje i CRM platforme. Integracija ovih sistema omogućava objedinjavanje podataka, automatizaciju procesa i smanjenje ručnog unosa informacija, čime se povećava efikasnost i smanjuje mogućnost grešaka (Laudon & Laudon, 2021; AIIM, 2021).

Za revizore, analiza integracije je ključna jer osigurava da se podaci tačno prenose između različitih sistema. Na primjer, ukoliko građanin podnese zahtjev putem e-portala, podaci o tom zahtjevu mogu se automatski prenijeti u centralni registar i sistem za obračun naknada. Revizor treba da provjeri da li se prenos podataka vrši u skladu sa definisanim pravilima, da li postoji audit trail za svaki transfer i da li su podaci konzistentni između sistema (ISACA, 2021).

Jedan od izazova integracije je očuvanje sigurnosti podataka tokom komunikacije između različitih sistema. To zahtijeva implementaciju sigurnih API-ja, enkripciju podataka i kontrolu pristupa na nivou sistema i korisnika. Revizori trebaju procijeniti da li su ove mjere implementirane i da li se periodično testiraju kako bi se osiguralo da integracija ne kompromituje bezbjednost podataka (ISO/IEC 27001, 2022).

Još jedna važna komponenta integracije je interoperabilnost – sposobnost različitih sistema da međusobno razmjenjuju podatke i da ih pravilno interpretiraju. U državnoj upravi to uključuje standardizovane formate podataka, upotrebu meta-podataka i implementaciju protokola koji omogućavaju nesmetanu razmjenu informacija između različitih odsjeka i agencija. Revizori trebaju provjeriti da li su korišćeni međunarodno prihvaćeni standardi i da li se podaci tačno i pravovremeno prenose.

Integracija e-portala sa drugim sistemima omogućava i naprednu analitiku i izvještavanje. Podaci iz različitih izvora mogu se kombinovati kako bi menadžment i revizori imali jasniji uvid u performanse državnih usluga, identifikovali potencijalne rizike i planirali unapređenja. Na primjer, integracija e-portala sa sistemom za upravljanje pritužbama građana omogućava praćenje efikasnosti rješavanja pritužbi i identifikaciju procesnih slabosti (Laudon & Laudon, 2021).

Efektivna integracija nije samo tehničko pitanje, već i pitanje upravljanja promjenama. Potrebno je obučiti zaposlene, definisati odgovornosti i procedure za korišćenje integrisanih sistema, te osigurati dokumentovanu kontrolu procesa. Revizori treba da provjere da li su ove procedure implementirane i da li se poštuju u praksi, jer to direktno utiče na pouzdanost i integritet podataka (ISACA, 2021).

Bezbjednost i kontrola pristupa u e-portalu

Jedan od najvažnijih aspekata e-portala u državnoj administraciji jeste bezbjednost podataka i kontrola pristupa. S obzirom da e-portali obrađuju osjetljive informacije o građanima, privredi i internim poslovnim procesima, zaštita tih podataka je od ključnog značaja kako bi se spriječile zloupotrebe, neovlašćeni pristupi ili gubitak informacija (ISO/IEC 27001, 2022).

Kontrola pristupa se obično implementira na više nivoa. Prvi nivo je autentikacija korisnika, koja uključuje provjeru identiteta putem korisničkog imena i lozinke, ali sve češće i dvofaktorsku autentikaciju (2FA) ili biometrijske metode, kao što su otisak prsta ili prepoznavanje lica. Drugi nivo predstavlja autorizaciju, koja definiše koje funkcionalnosti i podaci su dostupni određenim korisnicima ili grupama. Na primjer, građani mogu pristupiti samo svojim podacima i zahtjevima, dok službenici određene administrativne jedinice imaju pristup širem setu informacija u skladu sa svojom funkcijom.

E-portali takođe moraju obezbijediti audit trail – detaljno evidentiranje svih aktivnosti korisnika, uključujući vrijeme pristupa, vrste akcija i promjene podataka (ISACA, 2021). Ovi zapisi omogućavaju revizorima da prate tačnost i integritet procesa, identifikuju eventualne nepravilnosti i osiguraju odgovornost u radu službenika. Za revizore, analiza audit trail-a predstavlja ključni element procjene efikasnosti i sigurnosti e-portala, jer omogućava provjeru da li su procesi transparentni i u skladu sa zakonskim propisima.

Još jedan važan aspekt bezbjednosti jeste enkripcija podataka. E-portali moraju koristiti sigurne protokole (npr. HTTPS, TLS) za prenos podataka između korisnika i servera, kao i enkripciju podataka u bazi kako bi se zaštitile informacije u slučaju neovlašćenog pristupa (ISO/IEC 27001, 2022). Revizori treba da provjeravaju implementaciju ovih sigurnosnih mjera i njihovu efikasnost u praksi.

Implementacija politike bezbjednosti uključuje i redovno ažuriranje softvera, kontrolu pristupa administratora, reviziju logova i testiranje sistema protiv potencijalnih prijetnji, kao što su malware

ili pokušaji hakerskih napada. U praksi, revizori trebaju provjeriti da li su ove procedure formalno dokumentovane, primijenjene i da li se periodično revidiraju kako bi sistem ostao siguran i usklađen sa važećim standardima. Nakon cyber napada 2022. na IT infrastrukturu crnogorskih državnih institucija, naglasak je na obuci za cyber otpornost i periodično testiranje (e-Governance Academy, 2025).

Revizorski aspekti bezbjednosti e-portala

Revizori imaju ključnu ulogu u procjeni bezbjednosnih aspekata e-portala, jer pravilno implementirane kontrole smanjuju rizik od neovlašćenog pristupa, curenja podataka i drugih nepravilnosti (ISACA, 2021; ISO/IEC 27001, 2022).

1. Kontrola pristupa i autentikacija. E-portali koriste višeslojnu kontrolu pristupa kako bi osigurali da samo ovlašćeni korisnici imaju pravo da pristupe određenim funkcijama ili podacima. Autentikacija korisnika može biti zasnovana na lozinkama, tokenima, biometrijskim podacima ili digitalnim sertifikatima. Revizori trebaju procijeniti efikasnost ovih metoda, uključujući:
    - Provjeru da li su privilegije dodijeljene prema principu najmanjih privilegija.
    - Efikasnost mehanizama za promjenu lozinki, zaključavanje naloga i detekciju sumnjivih aktivnosti.
    - Postojanje audit trail-a koji evidentira sve pokušaje pristupa (ISO/IEC 27001, 2022).
2. Praćenje aktivnosti i audit trail. Audit trail omogućava praćenje svih aktivnosti korisnika unutar e-portala, uključujući prijave, izmjene podataka, odobravanja i druge akcije. Revizori koriste ove evidencije da:
    - Provjere usklađenost sa internim politikama i zakonskim zahtjevima.
    - Identifikuju nepravilnosti ili potencijalne zloupotrebe.
    - Testiraju efikasnost postojećih kontrola i sigurnosnih mjera (ISACA, 2021).
3. Zaštita podataka i enkripcija. E-portali moraju osigurati sigurnost podataka u tranzitu i u mirovanju koristeći napredne enkripcijske standarde. Revizori trebaju procijeniti:
    - Upotrebu HTTPS protokola i SSL/TLS enkripcije za komunikaciju između korisnika i servera.
    - Skladištenje podataka u šifrovanom obliku na serverima ili cloud platformama.
    - Upravljanje ključevima i pristupom enkripcijskim metodama (ISO/IEC 27001, 2022).
4. Usklađenost sa zakonodavstvom. E-portali moraju poštovati nacionalne i međunarodne zakone, uključujući GDPR ili lokalne zakone o zaštiti podataka, arhiviranju i reviziji dokumenata. Revizori provjeravaju:
    - Da li portal automatski primjenjuje zakonske rokove za čuvanje i uništavanje dokumenata.
    - Evidenciju saglasnosti korisnika za obradu njihovih ličnih podataka.

- Postojanje procedura za rješavanje zahtjeva korisnika vezanih za pristup, ispravku ili brisanje podataka (UN DESA, 2024).

5. Kontrole za kontinuitet poslovanja i oporavak od katastrofa. E-portali moraju imati planove za oporavak od incidenta i kontinuitet poslovanja, uključujući backup podataka, redundanciju servera i proceduru za hitni oporavak. Revizori provjeravaju:
    - Efikasnost i testiranost planova oporavka.
    - Periodičnu provjeru sigurnosnih kopija i integritet podataka.
    - Usklađenost sa preporukama za informatičku sigurnost i upravljanje rizicima (ISO 15489-1, 2016; ISACA, 2021).
6. Uloga e-portala u transparentnosti i reviziji. E-portali povećavaju transparentnost rada državnih organa jer omogućavaju:
    - Javni uvid u procedure i informacije o odobrenim zahtjevima.
    - Laku identifikaciju kašnjenja ili nepravilnosti u pružanju usluga.
    - Efikasnu pripremu podataka za revizorske izvještaje, jer svi relevantni događaji i dokumenti ostaju evidentirani u sistemu.

Kombinacija ovih funkcionalnosti i kontrola čini e-portale ključnim instrumentom za modernu, transparentnu i efikasnu upravu. Za revizore, sistematska procjena bezbjednosti, kontrole pristupa, audit trail-a i usklađenosti sa zakonskim propisima predstavlja osnovu za davanje objektivnih preporuka i povećanje povjerenja u digitalne sisteme državne uprave.

Uloga revizora u procjeni e-portala

Revizori u državnim organima imaju ključnu ulogu u procjeni pouzdanosti, sigurnosti i efikasnosti e-portala. Njihov zadatak je da osiguraju da sistem ispunjava svoje funkcionalne ciljeve, da su podaci tačni i integritet podataka zaštićen, te da su usluge dostupne korisnicima na siguran i transparentan način (ISACA, 2021).

Procjena pouzdanosti podrazumijeva provjeru da li e-portal omogućava tačan unos, obradu i pohranu podataka. Revizor provjerava da li su svi procesi vođeni prema definisanim procedurama, da li se zahtjevi korisnika pravilno registruju i obrađuju, te da li postoje mehanizmi za identifikaciju i ispravku grešaka.

Procjena sigurnosti obuhvata analizu kontrola pristupa, autentifikacije i zaštite podataka. Revizor ispituje da li su osigurani mehanizmi za zaštitu ličnih i osjetljivih podataka građana, kako je implementirana enkripcija komunikacije i pohrane podataka, te da li sistem evidentira sve aktivnosti kroz audit trail koji omogućava praćenje i identifikaciju eventualnih nepravilnosti (ISO/IEC 27001, 2022).

Procjena efikasnosti uključuje analizu da li e-portal omogućava pravovremenu i kvalitetnu obradu zahtjeva korisnika, smanjuje administrativno opterećenje i poboljšava dostupnost javnih usluga. Revizor provjerava workflow-e, integraciju sa drugim sistemima (ERP, CRM, eDMS) i automatizaciju procesa, te ocjenjuje da li su postignuti ciljevi uštede vremena i resursa (OECD, 2023).

Revizor koristi kombinaciju provjera, testiranja i analize dokumentacije kako bi ocijenio da li e-portal funkcioniše prema propisanim zahtjevima i standardima. Osim tehničkih kontrola, revizor procjenjuje i svijest korisnika i zaposlenih o sigurnom korišćenju sistema, što je posebno važno za smanjenje rizika od ljudskih grešaka ili neautorizovanog pristupa. U crnogorskom kontekstu revizori treba da prate implementaciju strategije digitalne transformacije za period 2022–2026, sa akcionim planom za 2024–2025, fokusirajući se na usklađenost sa EU kriterijumima (Ministarstvo javne uprave Crne Gore, 2022).

Na taj način revizor doprinosi osiguranju da e-portal bude pouzdan, siguran i efikasan alat u pružanju javnih usluga, a istovremeno da organizacija ostane u skladu sa zakonodavstvom i najboljim praksama u informacionoj sigurnosti i upravljanju IT sistemima.

5. Internet tehnologije kao podrška revizorskom poslovanju

Internet tehnologije predstavljaju ključni alat u savremenom revizorskom poslovanju. One omogućavaju efikasnije prikupljanje, obradu i analizu podataka, uz poboljšanu sigurnost i saradnju. Te tehnologije podržavaju prelazak sa tradicionalnih metoda na digitalne procese, uključujući automatizaciju, analitiku podataka i nadzor u realnom vremenu. To doprinosi većoj preciznosti i smanjenju rizika. Ovo poglavlje istražuje osnovne aspekte interneta i web-tehnologija, sa fokusom na njihovu primjenu u reviziji.

5.1. Uvod u internet i web-tehnologiju

Internet predstavlja globalnu mrežu računara povezanih kablovima, satelitima i bežičnim vezama. Ova mreža omogućava razmjenu informacija, komunikaciju i pristup raznovrsnim uslugama, uključujući društvene mreže, elektronsku poštu i web-sajtove. Internet funkcioniše tako što računari, telefoni ili tableti korisnika komuniciraju sa serverima, koji su moćni računari zaduženi za čuvanje podataka poput teksta, slika i videa. Svaki uređaj na internetu ima jedinstvenu IP adresu, poput 192.168.1.1, koja služi za identifikaciju. Sistem imena domena, poznat kao DNS, prevodi lako pamtljive adrese, poput „google.com“, u ove IP adrese kako bi se olakšao pristup web-sajtovima. Internet koristi protokole, poput HTTP ili HTTPS, za prenos podataka i TCP/IP za usmjeravanje informacija do pravog odredišta.

Da bi podaci putovali internetom, koriste se posebna pravila zvana protokoli. Protokol **TCP/IP (Transmission Control Protocol/Internet Protocol)** je skup pravila koja omogućavaju da podaci stignu do pravog odredišta pouzdano i bez grešaka. TCP dio ovog protokola razbija podatke na male djelove – pakete, i osigurava da svi stignu na pravo mesto u ispravnom redosljedu. Ako se neki paket izgubi, TCP ga ponovo šalje. IP dio protokola upravlja adresiranjem, odnosno usmjerava pakete do tačne IP adrese. Na primjer, kada pošaljete poruku preko interneta, TCP/IP osigurava da poruka stigne do primaoca, čak i ako putuje preko više računara i mreža. Još jedan važan protokol je **HTTP (HyperText Transfer Protocol)**, koji se koristi za prenos web-sajtova između servera i vašeg pregledača. Kada ukucate adresu web-sajta, HTTP šalje zahtjev serveru, koji zatim vraća podatke poput teksta i slika koje vidite na stranici. HTTPS je sigurnija verzija HTTP-a, koja koristi enkripciju da zaštiti podatke, poput lozinki ili brojeva kreditnih kartica, od neovlašćenog pristupa (Berners-Lee & Fischetti, 2001).

Web ili **World Wide Web (WWW)** je dio interneta koji koristimo preko web-pregledača, poput Chrome-a, Firefox-a ili Safari-ja, za posjetu web-sajtovima. Web-sajtovi se sastoje od stranica koje su međusobno povezane linkovima, koji omogućavaju prelazak sa jedne stranice na drugu jednostavnim klikom. Osnovne tehnologije za izradu web-sajtova uključuju HTML, CSS i JavaScript. **HTML**, što znači **HyperText Markup Language**, definiše strukturu web-stranice, uključujući naslove, paragrafe i linkove. **CSS** ili **Cascading Style Sheets** upravlja izgledom stranice, uključujući boje, fontove i raspored elemenata. **JavaScript** dodaje interaktivnost, poput dugmadi koja reaguju na klik ili animacija na stranici (Kurose & Ross, 2021).

Proces kreiranja web-sajta uključuje nekoliko koraka. Prvo, kreira se sadržaj koristeći HTML za strukturu, CSS za stil i JavaScript za funkcionalnost. Zatim se web-sajt postavlja na server kako bi bio dostupan na internetu. Da bi sajt bio javno dostupan, potrebno je kupiti domen, poput „mojsajt.me“, i uslugu hostinga, koja obezbjeđuje prostor na serveru. Internet i web-tehnologije omogućavaju dijeljenje znanja, globalnu komunikaciju, poslovne prilike poput elektronske trgovine i zabavu putem platformi za striming ili onlajn kurseve.

Internet i web-tehnologije, osim što omogućavaju komunikaciju i dostupnost informacija, postale su ključna infrastruktura savremenog poslovanja i javne uprave. Većina poslovnih procesa danas se odvija putem onlajn platformi, informacionih sistema povezanih internetom i web-aplikacija koje generišu digitalne evidencije.

Za revizore, ovo znači da tradicionalni pristup provjere papirne dokumentacije više nije dovoljan. Digitalno okruženje zahtijeva razumijevanje načina na koji funkcionišu internet protokoli, web-servisi, baze podataka i sigurnosni mehanizmi, jer se revizija sve više oslanja na analiziranje elektronskih zapisa, logova aktivnosti i tragova koje korisnici ostavljaju u sistemu.

Upravo zbog toga razumijevanje osnovnih internet i web-tehnologija predstavlja polaznu tačku za razumijevanje revizorskih postupaka u digitalnom okruženju.

5.2. Web-portal

Web-portal je posebna vrsta internet stranice koja služi kao centralna tačka pristupa različitim informacijama i uslugama. Možemo ga zamisliti kao ulaznu tačku za digitalne servise, gdje se na jednom mjestu nalaze različite funkcije – vijesti, pretraga, korisnički nalozi, formulari, servisi i drugi sadržaji (Berners-Lee & Fischetti, 2001). Za razliku od običnih web-stranica koje često imaju samo informativnu svrhu, portal je interaktivan i omogućava korisniku da komunicira sa sistemom, prilagođava prikaz sadržaja ili koristi određene elektronske usluge.

Primjer jednostavnog portala su početne stranice poput Google-a ili Yahoo-a, gdje sa jedne lokacije možete pristupiti pretrazi, e-pošti, mapama, vijestima i drugim alatima. Portal eUprava u Crnoj Gori funkcioniše na sličan način – građanin ne mora obilaziti različite institucije pojedinačno, već preko jednog portala može podnijeti zahtjev za dokument, platiti taksu ili dobiti informaciju o statusu predmeta.

Za razliku od običnog web-sajta koji može imati nekoliko statičnih stranica, portal integriše više funkcionalnosti i često omogućava personalizaciju sadržaja – na primjer, korisnik može izabrati koje vijesti želi da vidi ili da prati samo određene servise.

Da bi portal mogao da pruži sve te funkcije, u pozadini rade standardne web-tehnologije:

- HTML – postavlja strukturu stranice (meni, polje za prijavu, dio za vijesti),
- CSS – uređuje izgled i raspored elemenata kako bi portal bio pregledan,
- JavaScript – daje interaktivnost, na primjer automatsko osvježavanje informacija bez ponovnog učitavanja stranice.

Iza portala obično stoji serverska logika i baza podataka koja pamti korisničke naloge, zahtjeve, poruke ili istoriju korišćenja usluga.

Portali se mogu podijeliti prema svrsi:

- Javni portali – poput vladinih portala za građane (eUprava), koji nude elektronske usluge i informacije.
- Obrazovni portali – omogućavaju studentima pristup materijalima, testovima, komunikaciji sa nastavnicima.
- Korporativni portali – namijenjeni zaposlenima u organizaciji za internu komunikaciju i pristup dokumentaciji.
- Tematski/medijski portali – npr. portali sa vijestima, vremenskom prognozom, forumima i sličnim sadržajem.

Zajednička karakteristika svih portala je da spajaju više usluga i informacija na jednom mjestu, smanjujući potrebu da korisnik „luta“ internetom tražeći ono što mu treba.

Web-portali imaju ključnu ulogu u digitalizaciji usluga i administracije jer:

- olakšavaju građanima i korisnicima pristup informacijama,
- smanjuju potrebu za fizičkim odlaskom u institucije,
- omogućavaju centralizovan i pregledan sistem komunikacije i razmjene podataka,
- predstavljaju osnovu za dalji razvoj naprednih servisa poput elektronske revizije, praćenja zahtjeva u realnom vremenu i automatizovanih evidencija.

5.3. Web-pregledači

Web-pregledač (browser) je program koji koristimo za pregled internet sadržaja. To je alat kroz koji „ulazimo“ na internet, posjećujemo stranice, portale, prijavljujemo se na servise ili obavljamo elektronske transakcije. Najpoznatiji pregledači su Google Chrome, Mozilla Firefox, Microsoft Edge, Safari i Opera. Iako svaki izgleda vizuelno malo drugačije, njihova osnovna funkcija je ista – prikazivanje web-stranica na razumljiv i čitljiv način.

Bez pregledača korisnik ne bi mogao lako pristupiti sadržaju na internetu, jer su podaci na serverima zapakovani u tehničkim formatima (HTML, CSS, JavaScript) koje pregledač „prevodi“ u vizuelni prikaz koji vidimo na ekranu.

Pojednostavljeni proces funkcionisanja web-pregledača izgleda ovako:

- Korisnik unese adresu (npr. www.euprava.gov.me) u adresnu traku.
- Pregledač preko interneta šalje zahtjev serveru gdje se nalazi portal ili web-stranica.
- Server vraća potrebne podatke (kôd, slike, tekst).
- Pregledač obrađuje te podatke i prikazuje ih u obliku stranice koju korisnik vidi.

Pregledač takođe brine o sigurnosti prikaza – ako je stranica zaštićena HTTPS protokolom, on prikazuje ikonicu katanca koja znači da je komunikacija između uređaja i servera šifrovana.

Web-pregledači imaju niz funkcija koje su važne i iz ugla bezbjednosti i revizorskog posmatranja rada sistema, kao što su:

- Istorija pregleda (History) – čuva listu posjećenih stranica.
- Keš memorija – privremeno skladišti podatke kako bi se stranice brže učitale.

- Kolačići (Cookies) – male datoteke koje čuvaju korisničke postavke, prijave ili podatke o sesiji.
- Privatni/inkognito mod – omogućava pregled bez čuvanja istorije i kolačića.
- Notifikacije i dozvole – korisnik može dozvoliti ili zabraniti pristup lokaciji, kameri, mikrofonu, što je važno sa aspekta zaštite podataka.

Za revizora, web-pregledač nije samo alat za pristup sistemu, već i izvor podataka o ponašanju korisnika i potencijalnim bezbjednosnim rizicima. Na primjer:

- Pregledač može čuvati zapamćene lozinke, što predstavlja rizik ako uređaj koristi više osoba.
- Ako korisnici koriste zastarjele verzije pregledača, može postojati visok rizik od zloupotrebe zbog sigurnosnih propusta.
- Revizor može provjeriti da li korisnici pristupaju portalima preko sigurnih (HTTPS) ili nesigurnih veza.
- Analiza kolačića i keš memorije može pomoći u razumijevanju tragova korisničkih aktivnosti.

5.4. Internet podržana revizija

Razvoj internet tehnologija značajno je promijenio način na koji se obavljaju revizorski postupci, omogućavajući brži pristup podacima, automatizovanu analizu i efikasniju komunikaciju između revizora i klijenata. Tradicionalni revizorski proces, koji je podrazumijevao fizički uvid u dokumentaciju i ručnu provjeru evidencija, sve više se oslanja na digitalne platforme, elektronske baze podataka i onlajn komunikacione kanale (Braun & Davis, 2003).

Internet omogućava daljinski pristup knjigovodstvenim sistemima, što znači da revizori više ne moraju fizički biti prisutni kod klijenta da bi izvršili uvid u finansijske izvještaje ili pomoćnu dokumentaciju. Korišćenjem sigurnih web-portala, revizorske kuće organizuju razmjenu dokumentacije putem digitalnih „data room“ sistema, gdje klijent postavlja tražene dokumente, a revizor ih analizira uz mogućnost postavljanja dodatnih pitanja u realnom vremenu (INTOSAI, 2016).

Takođe, zahvaljujući internet tehnologijama, uobičajeni revizorski postupci kao što su testovi usklađenosti, analitičke procedure i potvrde stanja (eng. confirmations) sada se realizuju elektronskim putem. Na primjer, umjesto slanja fizičkih pisama bankama ili dobavljačima, revizori koriste elektronske potvrde (e-confirmations), čime se proces ubrzava i smanjuje rizik od falsifikovanja dokumentacije. ISA 505 standard zvanično uvodi mogućnost upotrebe elektronskih potvrda putem sigurnih internet kanala kao validnog revizorskog dokaza (IAASB, 2018).

Posebnu ulogu imaju onlajn analitički alati i softveri zasnovani na web-arhitekturi, koji omogućavaju automatsko prepoznavanje nepravilnosti u velikim skupovima podataka (tzv. big data auditing). Ovi alati koriste internet konekciju za integraciju sa ERP sistemima klijenata i omogućavaju kontinuiranu reviziju (eng. continuous auditing) – gdje se podaci analiziraju u realnom vremenu, a ne samo na kraju finansijskog perioda (Yoon, Hoogduin & Zhang, 2015).

Internet tehnologije su unaprijedile i komunikaciju u revizorskom timu, posebno kada se radi o međunarodnim projektima gdje članovi tima rade iz različitih zemalja. Onlajn platforme omogućavaju razmjenu nalaza, zajedničko pregledanje dokumenata i koordinaciju revizorskih aktivnosti.

Međutim, digitalizacija revizijskih procesa nosi i određene rizike. Pristup podacima preko interneta zahtijeva visok nivo informacione sigurnosti, enkripciju komunikacije i jasne kontrole pristupa kako bi se spriječile neovlašćene manipulacije podacima (Whitman & Mattord, 2021). Zbog toga savremeni revizor mora posjedovati informatičku pismenost i razumijevanje cyber rizika, jer revizija u digitalnom okruženju ne podrazumijeva samo provjeru finansijskih zapisa, već i razumijevanje IT kontrola koje štite integritet tih zapisa (ISACA, 2021). U tom smislu revizorska institucija je dužna da obezbijedi:

- enkriptovanu komunikaciju (SSL/TLS sertifikati),
- autentifikaciju korisnika putem višestruke verifikacije (MFA),
- jasno definisane nivoe pristupa kako bi se spriječilo da neovlašćena lica uđu u sistem,
- logovanje svih aktivnosti kako bi se u slučaju incidenta moglo utvrditi ko je pristupio kojim podacima.

Revizori procjenjuju i IT kontrole klijenta, jer ukoliko sistem nije dovoljno zaštićen, postoji rizik da finansijski podaci budu kompromitovani, što direktno utiče na kvalitet revizije.

6. Aplikativni softver kao podrška revizorskom poslovanju

Savremena revizija se više ne oslanja samo na računovodstvenu dokumentaciju u papirnom obliku, već se veliki dio revizorskih aktivnosti odvija u digitalnom okruženju. Priprema radnih papira, vođenje komunikacije sa kontrolisanim subjektom, analiza podataka i prezentacija nalaza danas se gotovo u potpunosti realizuju kroz standardne kancelarijske alate. Za razliku od klasičnih korisnika koji ove programe koriste za izradu dokumenata, revizor ih posmatra iz ugla sistema kontrole, dokaznih tragova i analitičkih tragova. Svaki dokument može predstavljati radni papir, svaka e-poruka može biti dokaz o komunikaciji, a svaka izmjena u tabeli može postati indikator manipulacije ili nepravilnosti. Zbog toga je važno razumjeti ne samo kako se ovi alati koriste, već kako se koriste na način koji podržava revizorsku metodologiju i čuva integritet podataka.

6.1. MS Word – tekst procesor u funkciji revizijske dokumentacije

MS Word je osnovni alat za pripremu radnih papira, nalaza i zvaničnih revizorskih izvještaja. Revizori ga koriste ne samo kao sredstvo za pisanje, već kao kontrolisani prostor dokumentovanja nalaza i evidentiranja tragova izmjena.

Za obnavljanje osnovnih funkcionalnosti možete koristiti priručnike za Word koji su dostupni na internetu (University of Nottingham, 2017; Wheaton Public Library, n. d.) (link na PDF u spisku literature). Ovdje ćemo razmotriti najvažnije funkcionalnosti za revizorsku praksu, kao što su:

- **Korišćenje unaprijed definisanih šablona** – revizorske institucije najčešće imaju standardne obrasce (radni list za kontrolu internih procedura, zapisnik o nalazu, izjava odgovornog lica), koji se u Word-u čuvaju kao predlošci (.dotx). Time se obezbjeđuje dosljednost i uporedivost dokumentacije.
- **Track Changes (Praćenje izmjena)** – svaka izmjena može biti vidljiva zajedno sa podacima o korisniku koji ju je načinio i vremenu izmjene. Ovo služi kao dokazni trag koji pokazuje kako je dokument evoluirao tokom revizije i sprečava nenajavljene prepravke.
- **Komentari i interna komunikacija u dokumentu** – revizorski timovi često ostavljaju komentare u marginama kao oblik interne konsultacije ili dodatnog objašnjenja. Time se izbjegava neformalna komunikacija van sistema i čuva audit trail unutar radnog papira.
- **Kontrola verzijā dokumenta** – posebno kada se dokumenti čuvaju u zajedničkom repozitorijumu (SharePoint, OneDrive for Business), Word omogućava pregled prethodnih verzija i vraćanje na stariju verziju ako je potrebno. Za revizora to znači da može dokazati kako je dokument izgledao u određenoj fazi procesa.
- **Zaštita dokumenta lozinkom ili zabrana izmjena** – kod osjetljivih nalaza moguće je zaključati dokument tako da se ne može uređivati bez ovlašćenja, čime se sprečava neovlašćeno mijenjanje radnih papira.

Tabela 8 prikazuje kako možete ove funkcionalnosti implementirati u Word-u.

Tabela 8. MS Word funkcionalnosti važne za reviziju

Funkcionalnost	Gdje se nalazi / kako se aktivira	Kratko objašnjenje
Korišćenje unaprijed definisanih šablona (.dotx)	*File → New → Personal / Custom Templates*	Revizorska institucija može unaprijed kreirati obrasce (radni listovi, zapisnici, izjave) koji se otvaraju kao novi dokumenti bez mijenjanja originalnog formata.
Track Changes (Praćenje izmjena)	*Review → Track Changes → Track Changes On*	Svaka izmjena se bilježi crvenom ili plavom oznakom, uz ime korisnika i tačno vrijeme izmjene – idealno za dokumentovanje toka revizije.
Komentari (Comments)	Označiti dio teksta → *Review → New Comment*	Revizorski tim može unositi interne napomene bez mijenjanja sadržaja dokumenta. Komentari ostaju kao dio audit trail-a.
Kontrola verzijā dokumenta (Version History)	Ako se dokument nalazi na OneDrive/SharePoint: Desni klik na fajl → *Version History*	Prikazuju se prethodne verzije dokumenta sa vremenskim oznakama. Revizor može dokazati kako je dokument izgledao u određenom momentu.
Zaštita dokumenta (Restrict Editing / Password Protect)	*File → Info → Protect Document → Restrict Editing* ili *Encrypt with Password*	Dokument se može zaključati tako da samo ovlašćeni članovi tima mogu uređivati sadržaj ili otvoriti fajl.

Na kraju, zaključujemo da pravilno korišćenje Word-a u revizorskoj praksi ne podrazumijeva napredno formatiranje, već kreiranje jasne, verzionisane i kontrolisane dokumentacije koja može biti prezentovana kao dokaz u postupku nadzora ili vanjske kontrole.

6.2. MS Excel

MS Excel je ključni alat za revizore kada je riječ o analizi podataka. Iako ga većina korisnika vidi kao tabelarni kalkulator, za revizora Excel predstavlja platformu za detekciju anomalija, obračune kontrolnih suma i provjeru dosljednosti evidencija.

Odličan priručnik za obnavljanje osnovnih funkcionalnosti Excela je autora Lambert and Frye, (2022) koji je dostupan na internetu (PDF dostupan na linku, vidi spisak literature). Ovdje ćemo istaći ključne funkcionalnosti relevantne za reviziju, kao što su:

- **Filtriranje i sortiranje podataka** – omogućava brzo otkrivanje nelogičnosti, kao što su:

    - transakcije bez datuma,
    - isplate bez naznačenog korisnika,
    - ponavljanje istog iznosa u kratkom periodu (indikator potencijalnog razbijanja transakcija).
- **Uslovno formatiranje (Conditional Formatting)** – koristi se za vizuelno označavanje rizika:
    - označavanje svih iznosa iznad određenog praga crvenom bojom,
    - vizuelno isticanje duplikata,
    - označavanje praznih ćelija u poljima koja moraju biti popunjena (npr. JMBG, IBAN, broj naloga).
- **Funkcije za kontrolu integriteta podataka** – Revizori često koriste funkcije kao što su:
    - COUNTIF – traženje duplikata ključeva (npr. isti broj fakture unijet dva puta).
    - VLOOKUP / XLOOKUP – provjera da li sve stavke iz pomoćne tabele (npr. lista transakcija) postoje i u glavnoj tabeli (na primjer lista korisnika).
    - SUMIF – provjera zbirnih iznosa po korisnicima, centrima troška ili projektima.
- **Pivot tabele (skrining velikih setova podataka)** – daju brz pregled strukture podataka po kategorijama. Revizor može, na primjer, za nekoliko sekundi vidjeti:
    - koji korisnik ima najveći broj naloga,
    - da li postoje korisnici sa samo jednom transakcijom (indikator fiktivnih unosa),
    - da li se pojavljuju neuobičajeni obrasci (npr. izuzetno veliki broj transakcija u neradnim danima).
- **Zaključavanje ćelija i zaštita radnih listova** – koristi se da bi se osiguralo da analitičke tabele ne budu naknadno mijenjane bez ostavljanja traga.
- **Audit Trail unutar Excel datoteka** – iako Excel nema napredne log sisteme kao baze podataka, revizor može koristiti sheet verzionisanje, kontrolne kolone (npr. „Unos izvršio“ ili „Datum revizorske provjere“), kao i funkcije za evidenciju izmjena kada se radi u okruženju kao što je SharePoint.

Funkcionalnosti Excela važne za reviziju i način njihovog aktiviranja date su u Tabeli 9.

Tabela 9. MS Excel funkcionalnosti važne za reviziju

Funkcionalnost	Kratko objašnjenje	Kako pristupiti / aktivirati u Excel-u
Filtriranje i sortiranje	Omogućava brzo pronalaženje nelogičnosti i analiziranje podataka po kolonama	Selektovati red sa naslovima kolona → kartica **Data** → **Sort** ili **Filter**
Uslovno formatiranje	Vizuelno ističe rizike: prazne ćelije, duplikate, iznose iznad praga	Selektovati ćelije → kartica **Home** → **Conditional Formatting** → odabrati pravilo (npr. Highlight Cells Rules / New Rule)

(Conditional Formatting)		
COUNTIF	Traženje duplikata ili broja pojavljivanja određenih vrijednosti	U praznu ćeliju unijeti formulu =COUNTIF(opseg, kriterijum)
VLOOKUP / XLOOKUP	Provjera postojanja vrijednosti u drugoj tabeli	=VLOOKUP(vrijednost, opseg_tabele, kolona, FALSE) ili =XLOOKUP(vrijednost, opseg_traženja, opseg_za_vraćanje)
SUMIF	Provjera zbirnih iznosa po korisnicima, projektima ili centrima troška	=SUMIF(opseg_kriterijuma, kriterijum, opseg_sumiranja)
Pivot tabele	Brzi pregled strukture podataka i identifikacija neuobičajenih obrazaca	Selektovati opseg → kartica **Insert** → **PivotTable** → odabrati lokaciju i polja
Zaključavanje ćelija / zaštita sheet-a	Sprečava neovlašćene izmjene u analitičkim tabelama	Selektovati ćelije → desni klik → **Format Cells** → **Protection** → označiti „Locked“ → kartica **Review** → **Protect Sheet**
Audit Trail / verzionisanje	Evidencija izmjena unosa u Excel-u, bilježenje ko je i kada mijenjao podatke	Ako se koristi SharePoint / OneDrive → desni klik na fajl → **Version History**; dodatno, kreirati kolone „Unos izvršio“, „Datum provjere“

Excel je najčešće prvi alat koji revizor otvara nakon preuzimanja podataka iz sistema. Korišćenjem sistematskog analitičkog pristupa Excel postaje alat za rano otkrivanje rizika i selekciju uzoraka za detaljnu reviziju.

Tako recimo, za primjer relacione baze podataka iz sekcije 2.1, **fiktivni zaposleni** 2007 koji radi na projektu P001, a ne postoji u tabeli Zaposleni, može se otkriti pomoću **VLOOKUP**.

Pretpostavimo da su relacione tabele izvezene u Excel i da se svaka tabela nalazi od početka posebnog Sheet-a imenovanog po nazivu tabele:

Sheet	**Početak**	**Struktura**
Zaposleni	A1	ID_ZAPOSLENOG, Ime i prezime, JMBG, ID_ODSJEKA
Projekti	A1	ID_PROJEKTA, Naziv projekta
Zaposleni_Projekat	A1	ID_ZAPOSLENOG, ID_PROJEKTA

Na Sheet-u Zaposleni_Projekat u C1 unesemo naziv kolone **Postoji u Zaposleni?**

U C2 unesemo formulu **=VLOOKUP(A2, Zaposleni!A:D, 1, FALSE)** i iskopiramo u ostala polja kolone C. Parametri unutar funkcije imaju sljedeće značenje:

- A2 = ID_ZAPOSLENOG iz tabele Zaposleni_Projekat
- Zaposleni!A:D = opseg tabele u Sheet-u Zaposleni (kolona A je ID_ZAPOSLENOG, kolona D je ID_ODSJEKA)
- 1 = vraća vrijednost iz 1. kolone opsega (ID_ZAPOSLENOG)
- FALSE = traži tačno podudaranje

Ako VLOOKUP pronađe ID vraća ID, ako ne pronađe ID vraća #N/A. Dakle, rezultat je sljedeći:

ID_ZAPOSLENOG (A)	**ID_PROJEKTA (B)**	**Postoji u Zaposleni? (C)**
2001	P001	2001
2001	P002	2001
2002	P001	2002
2007	**P001**	**#N/A**

Zaključak na osnovu rezulata je da zaposleni **2007** radi na projektu **P001**, ali **NE POSTOJI u tabeli Zaposleni.** Ovo je „viseći“ spoljnji ključ → indikator fiktivnog zaposlenog ili ručnog unosa mimo sistema.

6.3. MS Outlook

MS Outlook nije samo alat za slanje e-pošte – u revizorskom procesu on ima ulogu evidencijskog i kontrolnog sistema komunikacije, jer svaka poruka, prilog ili potvrda može predstavljati revizorski dokaz.

Osnovne funkcionalnosti ovog alata se mogu maći u Microsoft-ovom step-by-step priručniku (Lambert, 2016) (PDF dostupan na linku, vidi spisak literature). Ključne funkcionalnosti relevantne za revizora su:

- Strukturirano vođenje komunikacije sa klijentima
    - Kreiranje posebnih foldera po revizorskim predmetima (npr. *Revizija Budžetskog korisnika 2024 – Komunikacija*).
    - Razdvajanje zvaničnih potvrda i radne komunikacije.
    - Pravilo: *„Ako nije evidentirano u komunikaciji, smatra se da nije zatraženo“.*
- Korišćenje „Request a Read Receipt“ i „Delivery Receipt“ funkcije
    - Revizor može zahtijevati dokaz da je dokument (npr. zahtjev za izvještaj o transakcijama) zvanično dostavljen i pročitan.
    - Ove potvrde se čuvaju kao dokaz profesionalne komunikacije i pravovremenog traženja dokumentacije.

- Integracija e-maila sa rokovima (kalendar i task menadžment)
    - Poruku koja sadrži obavezu (npr. *„Dokumentacija će biti dostavljena do petka“*) revizor može pretvoriti direktno u task sa podsjetnikom.
    - Na ovaj način se izbjegava rizik gubitka rokova ili zaboravljenih zahtjeva.
- Kategorizacija i označavanje prioritetnih komunikacija
    - Revizor označava crvenim markerom e-poruke koje sadrže kritične informacije ili potvrde trećih strana (banke, dobavljači, druge institucije).
    - Ovaj način vizuelnog upravljanja inboxom omogućava da bitni dokazi ostanu lako dostupni prilikom pisanja završnog izvještaja.
- Arhiviranje i pravna relevantnost
    - Poruke u Outlooku mogu se izvesti u PDF ili .msg formatu i arhivirati uz revizorsku dokumentaciju.
    - U pojedinim revizorskim standardima priznaje se elektronska korespondencija kao validan revizorski dokaz, pod uslovom da se čuva u autentičnom obliku.
- Sigurnosni aspekt
    - Revizor treba da obrati pažnju na phishing i lažne e-mailove, posebno kada elektronski prima dokumente ili potvrde od trećih strana.
    - Outlook omogućava označavanje sumnjivih poruka i blokiranje neovlašćenih pošiljalaca, što je važno za očuvanje integriteta revizorskog procesa.

Uputstva za aktivaciju i podešavanje ovih funkcionalnosti u alatu navedena su u Tabeli 10.

Tabela 10. MS Outlook funkcionalnosti važne za reviziju

Funkcionalnost	**Korisničko uputstvo u MS Outlook-u**
Kreiranje foldera po revizorskim predmetima	Desni klik na Inbox → New Folder → unijeti naziv (npr. „Revizija Budžetskog korisnika 2024 – Komunikacija“).
Razdvajanje zvaničnih potvrda i radne komunikacije	Napraviti podfoldere unutar glavnog foldera („Zvanične potvrde“, „Radna komunikacija“).
Korišćenje „Request a Read Receipt“	Prilikom slanja e-maila: Options → Request a Read Receipt.
Korišćenje „Delivery Receipt“	Prilikom slanja e-maila: Options → Request a Delivery Receipt.
Pretvaranje poruke koja sadrži obavezu u task	Desni klik na poruku → Move → Tasks ili drag & drop u Tasks → Postaviti podsjetnik.
Kategorizacija i označavanje poruka (boje/prioritet)	Desni klik na poruku → Categorize → odabrati boju (npr. crvena za kritične informacije).

Vizuelno upravljanje inboxom (Conditional Formatting)	View → View Settings → Conditional Formatting → Dodati pravilo za boje i prioritet.
Arhiviranje poruka u PDF ili .msg	File → Save As → odabrati PDF ili Outlook Message Format (.msg).

Outlook u revizorskom radu postaje digitalni dnevnik komunikacije i alat za upravljanje dokazima, a pravilna struktura inboxa i arhive često pravi razliku između dobro dokumentovane revizije i one u kojoj se tragovi dokaza gube.

6.4. MS PowerPoint

MS PowerPoint je alat koji revizori koriste u završnoj fazi procesa – prilikom prezentacije ključnih nalaza, preporuka i identifikovanih rizika upravi, odboru direktora ili nadzornim organima. Za razliku od Worda i Excela, koji služe za detaljnu dokumentaciju, PowerPoint se koristi za strateško i jasno saopštavanje suštine.

Revizor koristi PowerPoint u praksi za:

- **Pripremu završne prezentacije nalaza**
  - Umjesto čitanja kompletnog nalaza, uprava očekuje sažetak ključnih rizika, nepravilnosti i preporuka.
  - PowerPoint omogućava vizuelnu prezentaciju nalaza kroz grafikone, infografike i numeričke pokazatelje.
- **Strukturiranje prezentacije po logici revizorskih izvještaja**
  - Uvod: *Cilj revizije i obuhvaćeni procesi*
  - Identifikovani rizici: *npr. loša kontrola pristupa u bazi podataka, neusklađeni zapisi u ERP sistemu*
  - Dokazi i primjeri: *isječci ekrana, tabele iz Excela, grafikoni*
  - Preporuke: *jasno definisane aktivnosti i odgovorne osobe*
  - Zaključak: *procjena zrelosti kontrolnog sistema i naredni koraci*
- **Korišćenje vizuelnih elemenata za jači uticaj**
  - Grafikoni (npr. „Broj korisnika bez MFA zaštite“)
  - Piktogrami za označavanje nivoa rizika (nizak / srednji / visok)
  - Boje za signalizaciju – u revizorskim prezentacijama često se koristi zeleno (usaglašeno), žuto (potrebno unapređenje), crveno (kritično stanje)

PowerPoint je važan za reviziju jer:

- Rukovodstvo često nema vremena da čita detaljan narativni izvještaj
- Prezentacija omogućava direktnu diskusiju o ključnim nepravilnostima
- Dobro strukturirane revizorske prezentacije pojačavaju autoritet nalaza i olakšavaju implementaciju preporuka.

Efikasna revizorska prezentacija treba da slijedi preporuke prikazane u Tabeli 10.

Tabela 10. Preporuke za elemente revizorske prezentacije

Element	**Revizorska preporuka**
Naslovi slajdova	Neka izražavaju zaključak, ne samo temu (npr. umjesto *„Kontrola pristupa“*, piše *„15% korisnika ima neograničen pristup bez revizije logova“*)
Tekst	Koristiti **kratke poruke i liste**, ne pasuse
Brojevi	**Naglasiti procentualne pokazatelje i trendove**, jer oni ostavljaju jači utisak na rukovodstvo
Rizici	**Vizuelno označiti nivo rizika** (ikonama ili bojom)
Preporuke	**Konkretnost: ko, šta, do kada** — bez opštih fraza tipa „poboljšati sistem kontrola“

MS PowerPoint je ključan alat za komunikaciju revizorskih nalaza prema donosiocima odluka, jer pomaže da se tehničke i kompleksne informacije prikažu jasno, sažeto i strateški – što direktno utiče na prihvatanje i implementaciju preporuka.

Uputstvo za upotrebu ovog alata se može naći na linku u spisku literature (Lambert, 2015).

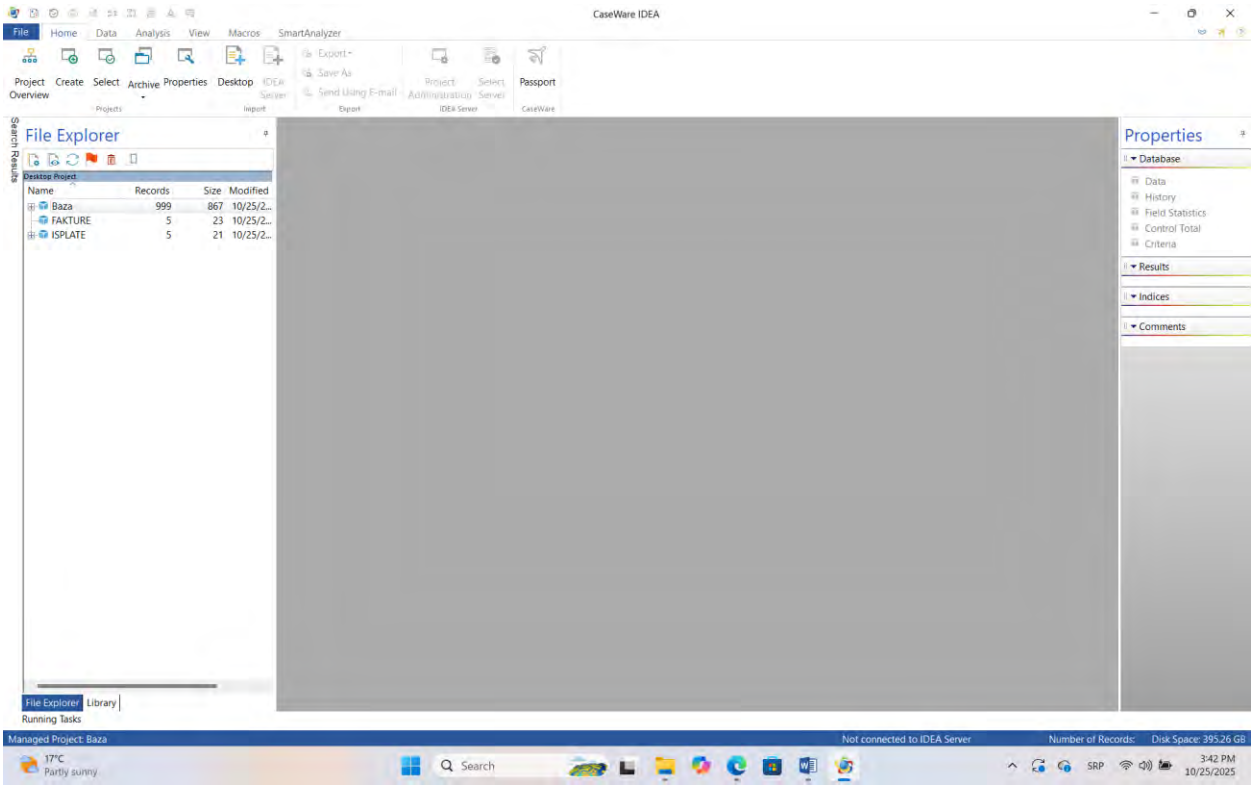
7. Specijalizovani softver za reviziju – IDEA softver za analizu podataka

7.1. Opšte informacije

IDEA (Interactive Data Extraction and Analysis) je specijalizovani softver koji je razvila kompanija **CaseWare Analytics**. Koristi se u finansijskoj reviziji, internoj reviziji i kontrolama, forenzičkoj analizi i opštem poslovnom nadzoru. Osnovna svrha IDEA-e jeste da omogući **efikasnu analizu velikih skupova podataka** bez potrebe za ručnim pretraživanjem i obradom u tabelama.
Softver omogućava revizorima i analitičarima da:

- ispituju integritet i tačnost podataka,
- prepoznaju nepravilnosti, duplikate i greške,
- izvode statističke i računovodstvene testove,
- izvještavaju rezultate u obliku kojih je spreman za dokumentaciju revizije.

IDEA verzija 10 (CaseWare IDEA Inc, 2018) ima moderan interfejs sličan MS Office-u (ribbon alatna traka) (vidi Sliku 13), što omogućava intuitivno korišćenje i lak prelazak s Excel-a na ovaj profesionalni alat za reviziju podataka.



Slika 13. Glavni interfejs IDEA 10 (ribbon traka i prozori)

7.2. Glavne karakteristike

IDEA 10 sadrži niz funkcionalnosti koje pokrivaju čitav ciklus revizijske analize podataka:

- **Uvoz podataka** iz različitih formata: Excel, CSV, Access, text, PDF, SAP, SQL baze, i drugih računovodstvenih sistema.
- **Sigurnost i integritet** – svi podaci se čuvaju u originalnom obliku; IDEA ne mijenja izvorni fajl već kreira novu kopiju baze.
- **Audit trail (trag revizije)** – svaka izvršena radnja automatski se evidentira u *History* prozoru i može se kasnije pregledati ili dokumentovati.
- **Rad sa velikim bazama** – podržava stotine hiljada redova bez pada performansi.
- **Automatizacija analiza** – mogućnost kreiranja skripti (IDEAScript) i ponavljanja analiza na novim setovima podataka.
- **Statističke i računovodstvene funkcije** – uključuju sumarizaciju, ekstrakciju, stratifikovanje, uzorkovanje, istraživanje podataka poput detekcije praznina ili dupliranih ključeva u podacima.
- **Vizuelni prikaz rezultata** – rezultati analiza mogu se prikazati kao tabele, grafikoni, pivot prikazi ili izvesti u Excel / PDF.

Program se sastoji od više **prozora (windows)** koji služe za pregled i analizu podataka (vidi Sliku 14). Svaki prozor ima određenu funkciju i mogu se otvoriti, zatvoriti ili premještati po želji. Najvažniji prozori u aplikaciju su:

1. Database Window (Prozor baze podataka)

- Prikazuje podatke u tabeli – svako polje (kolona) ima naziv, a svaki red predstavlja jedan zapis (record).
- Može biti istovremeno otvoreno više baza, svaka u svom prozoru.
- Naziv aktivne baze se vidi u naslovnoj traci programa.

2. Properties Window (Prozor s osobinama)

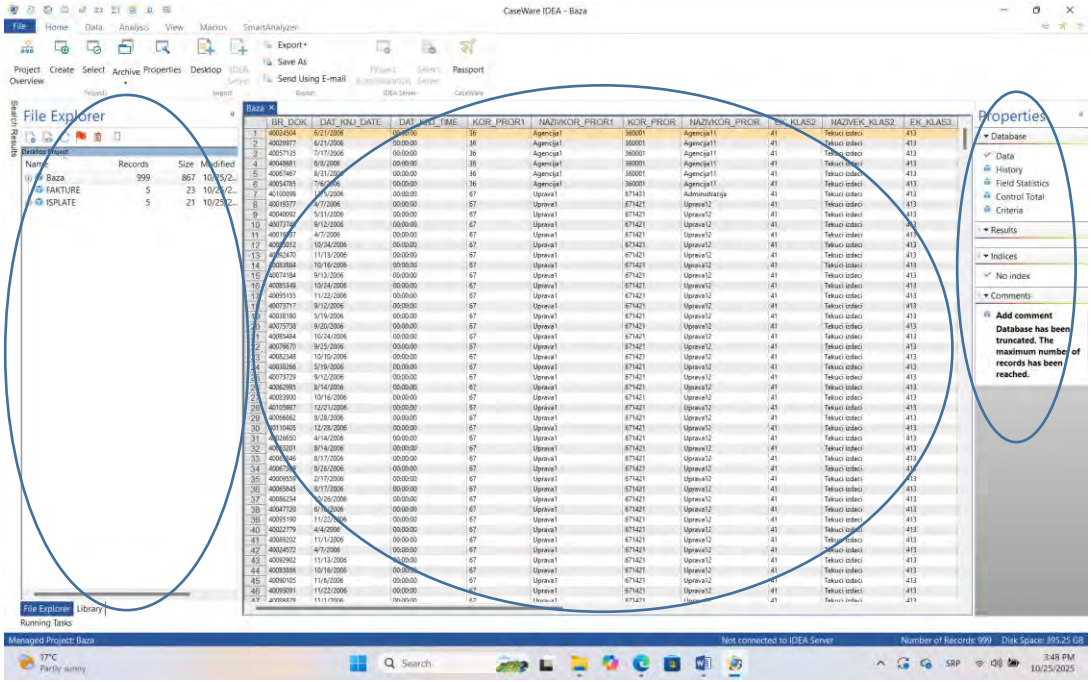
Prikazuje različite informacije o aktivnoj bazi:

- **Data** – prikaz podataka kao u Excelu
- **History** – prikazuje sve korake koje si uradio u toj bazi
- **Field Statistics** – statistike o kolonama (broj, prosjek, maksimum...)
- **Control Total** – sabira vrijednosti izabranog polja (npr. ukupna prodaja)
- **Criteria** – prikazuje uslove (filtere) koji su primijenjeni
- **Results** – pokazuje rezultate analiza
- **Indices** – prikazuje redosljed sortiranja
- **Comments** – omogućava dodavanje bilješki

3. File Explorer Window (Istraživač datoteka)

- Slično kao Windows Explorer – prikazuje sve baze i fajlove u projektu.
- Mogu se kreirati podfolderi, brisati, preimenovati ili označavati baze.
- Prikazuje broj zapisa, veličinu fajla i datume izmjene.

Ako se raspored prozora poremeti, uvijek se može vratiti na početne postavke preko **View → Restore Default Layout**.

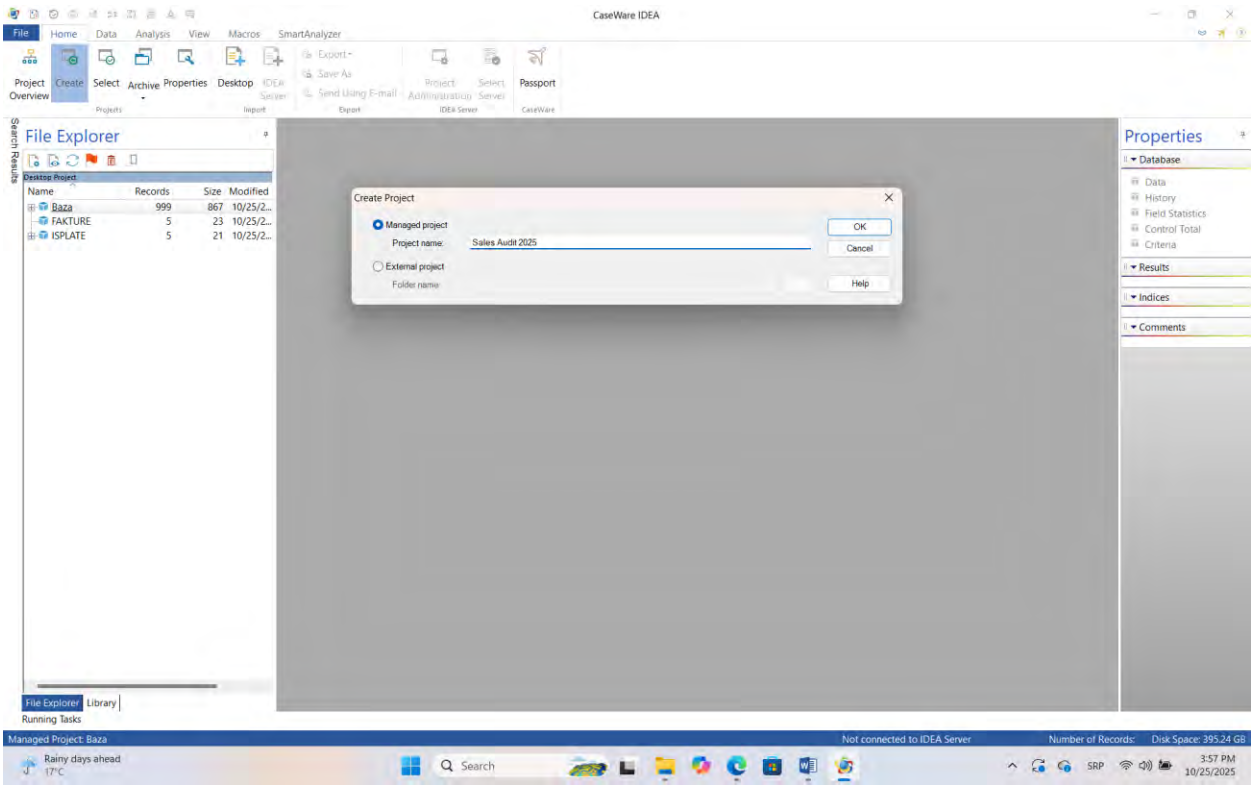


Slika 14. File Explorer, Database Window i Properties Window

Rad u programu korisnik započinje **kreiranjem projekta**, na sljedeći način:

- Na vrhu ekrana kliknuti na **Home** (Početna) karticu
- U grupi **Projects** kliknuti na dugme **Create** (vidjeti Sliku 15)
- U polje **Project name** upisati ime projekta (npr. *Sales Audit 2025*)
- Kliknuti **OK**.
- Novi projekat se otvara, ali **File Explorer** je prazan jer još nijesu dodate baze podataka. Projekat je kreiran na standardnoj lokaciji u folderu *Documents/My IDEA Documents/IDEA Projects*.

Nakon toga mogu se uvoziti podaci (npr. Excel, Access, tekstualni fajlovi) i započeti analiza.

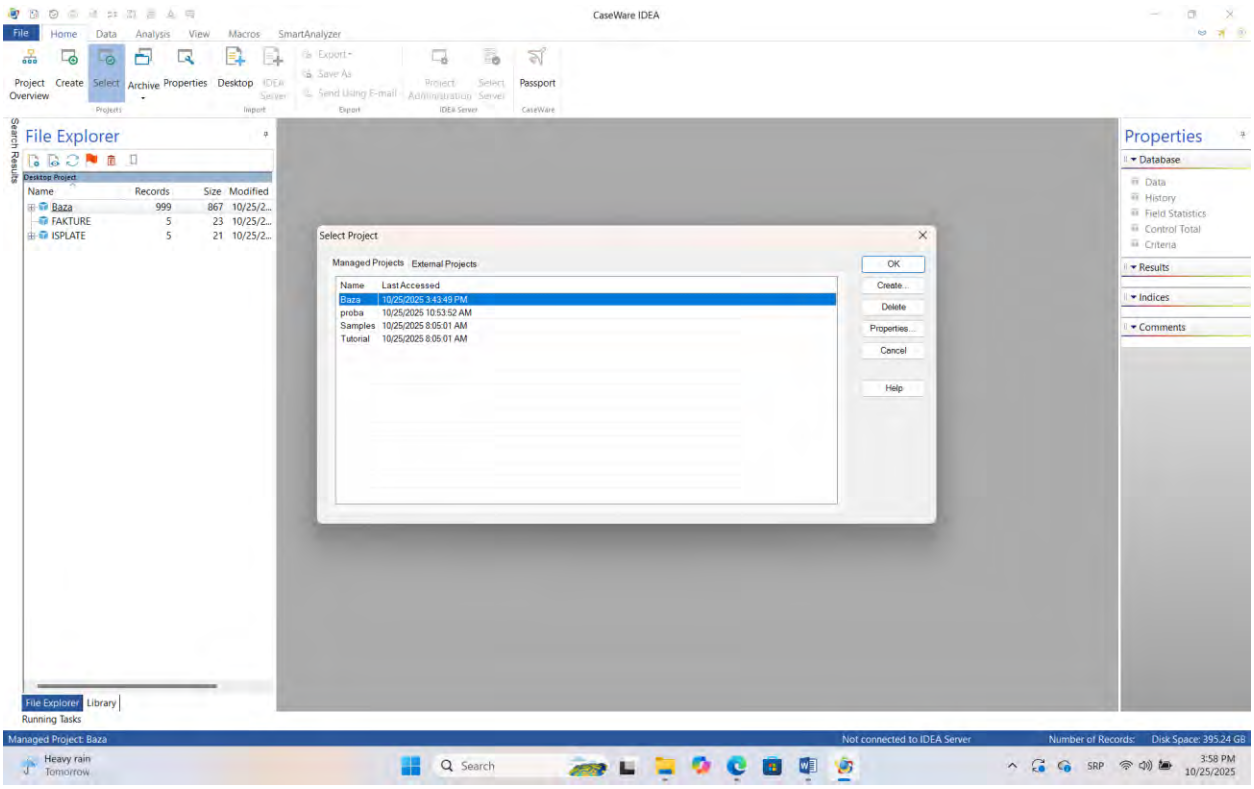


Slika 15. Dijalog za kreiranje novog projekta

Za **selekciju ili brisanje postojećeg projekta** postupak je sljedeći:

- Na kartici **Home**, u grupi **Projects**, kliknuti na **Select**.
- U prozoru koji se otvori odabrati karticu **Managed Projects** (ukoliko su projekti sačuvani na standardnoj lokaciji) (vidi Sliku 16).
- Prikazuje se lista postojećih projekata (npr. Tutorial, Samples).
- Za otvaranje projekta kliknuti na željeni projekat i zatim na **OK**.
- Naziv aktivnog projekta prikazan je u donjem lijevom uglu ekrana (npr. Managed Project: Tutorial).
- **File Explorer** prikazuje sve baze podataka koje pripadaju izabranom projektu.
- Za brisanje projekta kliknuti na željeni projekat a zatim na opciju **Delete** i potvrditi na **Yes**.
- U **File Exploreru** će nestati baze podatka koje pripadaju izbrisanom projektu.

IDEA može imati aktivan samo jedan projekat u datom trenutku. Prilikom otvaranja novog projekta, prethodni se automatski zatvara.



Slika 16. Dijalog za selekciju postojećeg projekta

Baze podataka koje pripadaju projektu mogu se u **File Exploreru** direktno **brisati** ili **preimenovati** koristeći desni klik na izabranu bazu.

7.3. Ispitivanja

U revizijskoj praksi IDEA omogućava izvođenje širokog spektra **ispitivanja** (analitičkih testova) nad finansijskim i operativnim podacima. Najčešće vrste ispitivanja uključuju:

- **Test potpunosti i tačnosti** – provjerava da li su svi podaci unijeti i da li postoje numeričke greške.
- **Test duplikata (Duplicate Key Detection)** – pronalazi duple zapise, npr. ponovljene fakture ili isplate.
- **Test sekvenci (Gap Detection)** – otkriva nedostajuće brojeve faktura, čekova ili naloga.
- **Analiza iznosa (Stratification / Summarization)** – grupisanje i sumiranje podataka prema odabranim kriterijumima.
- **Ekstrakcija (Extract)** – izdvajanje zapisa koji ispunjavaju određene uslove, npr. „iznosi veći od 10.000 €“.
- **Statističko uzorkovanje (Random Sampling)** – izbor slučajnog uzorka za detaljnije ispitivanje.
- **Kontrolni proračuni (Control Totals)** – provjeravaju da li zbir određenih polja odgovara knjigovodstvenim zapisima.

Ovi testovi omogućavaju revizoru da potvrdi pouzdanost i integritet podataka prije davanja revizijskog mišljenja.

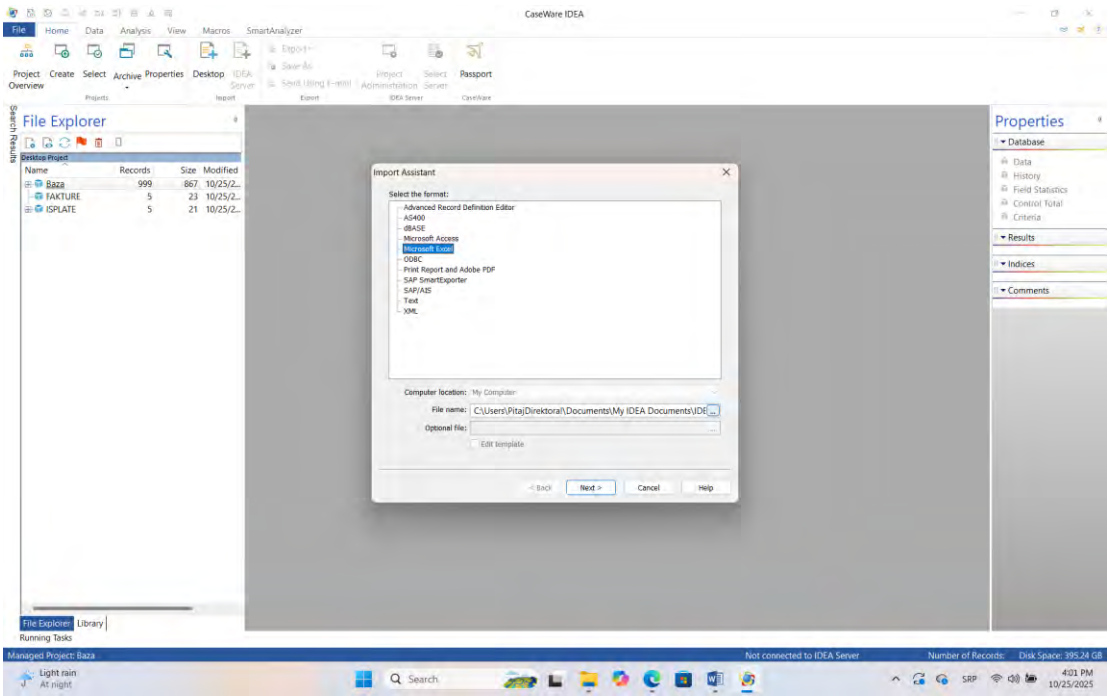
7.4. Podaci

U IDEA-i se svi uvezeni podaci organizuju u **baze (databases)**. Svaka baza sadrži **polja (fields)** koja mogu biti različitih tipova:

- **Numeric (numerička)**,
- **Date (datumska)**,
- **Character (tekstualna)**,
- **Time (vremenska)**,
- **Boolean (logička: tačno/netačno)**.

Uvoz podataka je prvi korak u radu sa IDEA projektom. Postupak se izvodi na sljedeći način:

- Na kartici **Home**, u grupi **Import**, kliknuti **Desktop**.
- U listi formata izabrati tip fajla (npr. Excel, Text, Access) (vidi Sliku 17).
- Kliknuti na **(...)** desno od **File name** i pronaći datoteku koja se uvozi.
- Kliknuti **Open**, a zatim **Next**.
- IDEA prikazuje pregled podataka i automatski određuje tipove polja i njihovu dužinu.
- U posljednjem koraku unijeti ime baze (**File name**) i kliknuti **Finish**.
- Nova baza podataka pojavljuje se u **File Explorer** prozoru i može se otvoriti za pregled u **Database Window**-u.

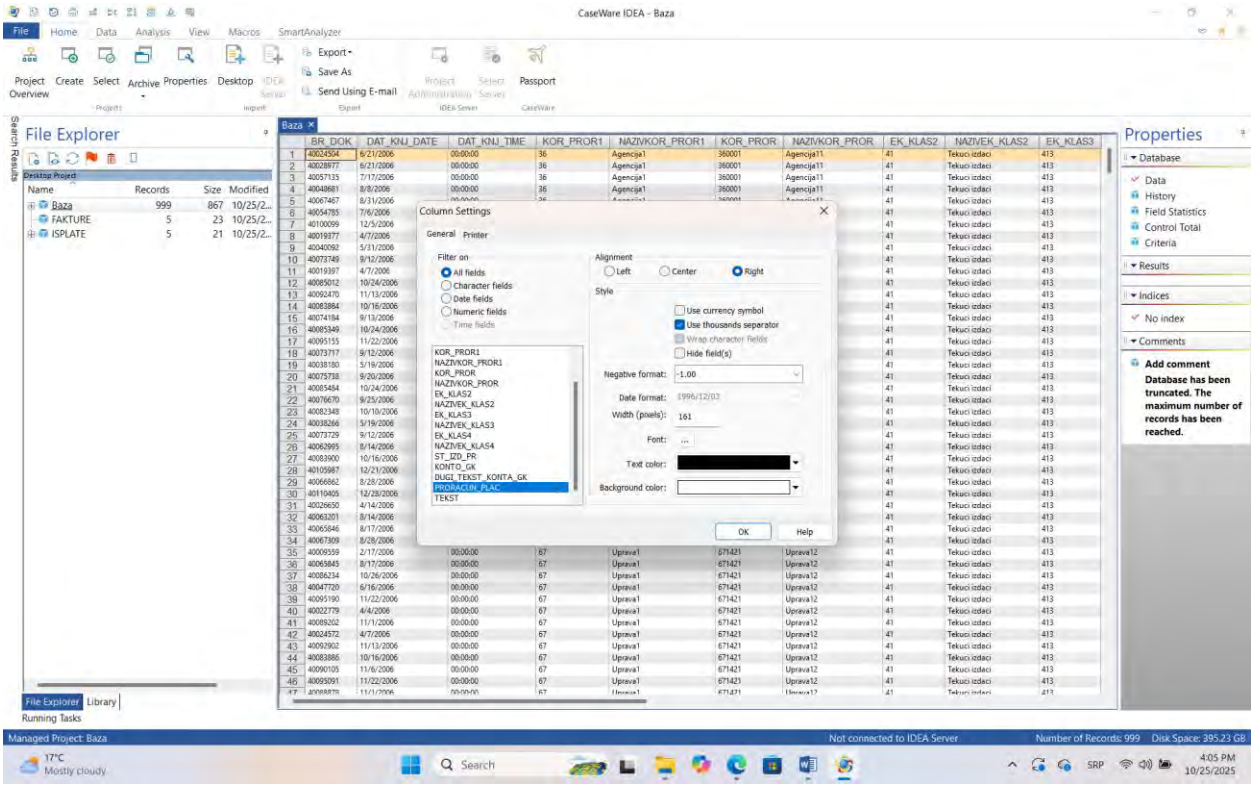


Slika 17. Uvoz Excel fajla

Podaci se u prozoru **Database Window**, mogu **formatirati**, odnosno mogu se prilagođavati načini prikaza i redosljeda kolona. Formatiranje ne mijenja izvorne podatke, već samo način na koji su prikazani u bazi. Postupak formatiranja se može izvesti na sljedeće načine:

- Postaviti pokazivač miša na granicu između zaglavlja kolona i povlačenjem **promijeniti širinu kolone**.
- Dvoklikom na naziv kolone **sortirati zapise** u rastućem ili opadajućem redosljedu (pored naziva se pojavljuje strelica koja označava redosljed).
- Desnim klikom na zaglavlje kolone izabrati **Column Settings...** (vidi Sliku 18) da bi se promijenio prikaz podataka:
    - boja teksta i pozadine,
    - podebljan prikaz (bold),
    - prikaz u valuti ili sa separatorima hiljada (za numerička polja).
- **Kolone se mogu premještati** tako što se klikne na zaglavlje kolone i prevuče na željenu poziciju (IDEA prikazuje crvenu liniju na mjestu gdje će kolona biti postavljena).
- Na kartici **View**, u grupi **Views**, moguće je kliknuti **Reset** da bi se poništile sve promjene i vratio početni izgled tabele.

Ove opcije formatiranja pomažu u vizuelnom sređivanju baze i olakšavaju dalju analizu, bez uticaja na izvorne vrijednosti u datoteci.



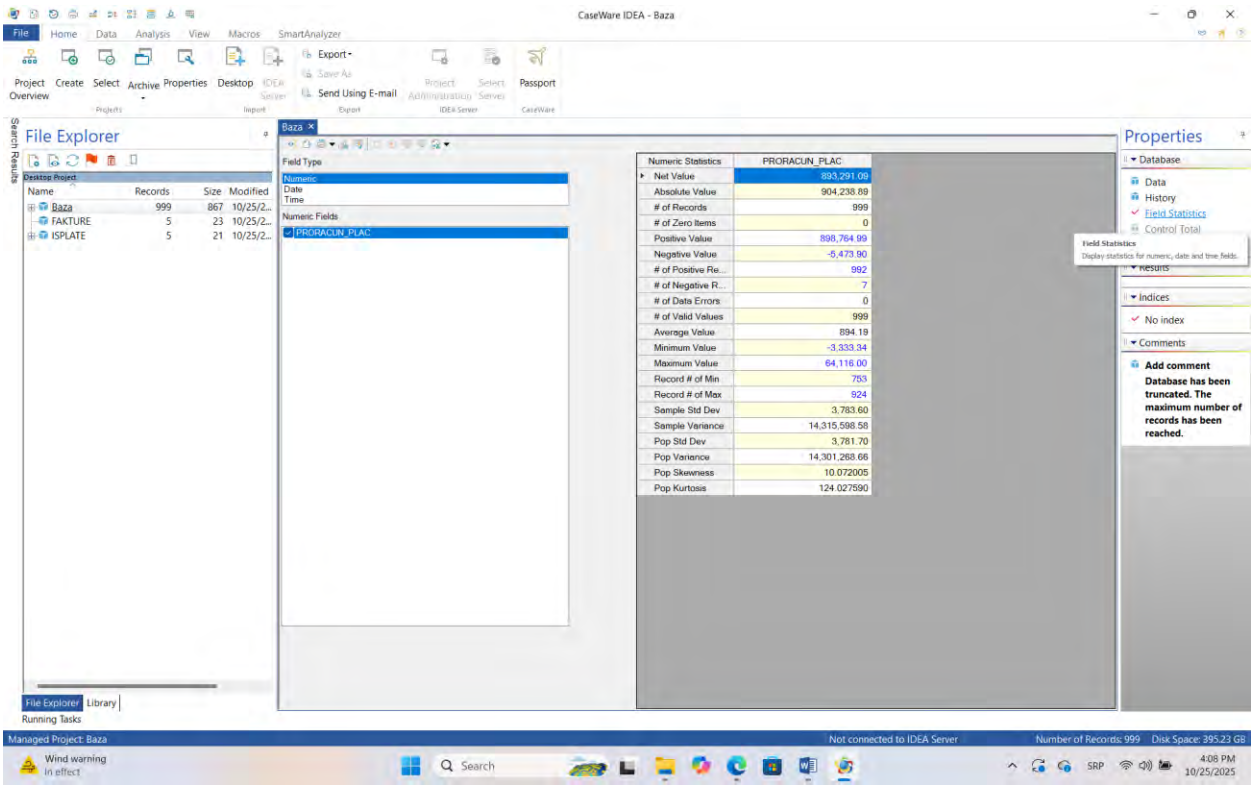
Slika 18. Column Settings dijalog za formatiranje kolona

IDEA omogućava automatsko generisanje **statistike (Field Statistics)** za numerička, datumska i vremenska polja u bazi podataka. Ova funkcija pomaže da se brzo identifikuju odstupanja,

ekstremne vrijednosti i mogući problemi u podacima prije izvođenja složenijih analiza. Postupak je sljedeći:

- Otvoriti bazu podataka u **Database Window**.
- U **Properties** prozoru kliknuti na karticu **Field Statistics** (vidi Sliku 19).
- IDEA će ponuditi opciju da automatski izračuna statistike za polja – potvrditi izbor klikom na **Yes**.
- Izabrati **Field Type** tj. koja polja želite analizirati, numerička ili datumska. Zatim čekirati polje za koje želite da vidite statistiku.
- U prikazu **Field Statistics** prikazuju se osnovni pokazatelji za numeričko polje, kao što su:
    - **# of Records** – broj zapisa u koloni,
    - **# of Zero Items** – broj nula u koloni,
    - **Minimum / Maximum** – najmanja i najveća vrijednost,
    - **Mean / Median** – aritmetička sredina i medijana,
    - **Standard Deviation** – odstupanje od prosjeka,
    - **Total** – zbir vrijednosti.
- Klikom na vrijednost sa desne strane pokazatelja označenu plavom bojom (npr. pored pokazatelja *Maximum Value*) IDEA automatski otvara zapis u kojem se ta vrijednost nalazi.
- Klikom na neke vrijednosti može se otvoriti više zapisa u vezi te vrijednosti (npr. pored pokazatelja *# of Negative Records*).
- Za datumsko polje prikazuju se pokazatelji, kao što su:
    - **Earliest/Latest Date** – najraniji i najkasniji datum
    - **Most Comon Day/Month** – najčešći dan i mjesec
    - **Items in January/February,...** – broj transakcija u mjesecu
    - **Items on Sunday/Monday,...** – broj transakcija po danu
- Povratak na prikaz tabele podataka vrši se izborom opcije **Data** u **Properties** prozoru.

Field Statistics funkcionalnost omogućava brzu provjeru kvaliteta i tačnosti podataka, kao i otkrivanje nepravilnosti, poput nelogično visokih iznosa, neuobičajenih vremenskih trendova ili negativnih vrijednosti.

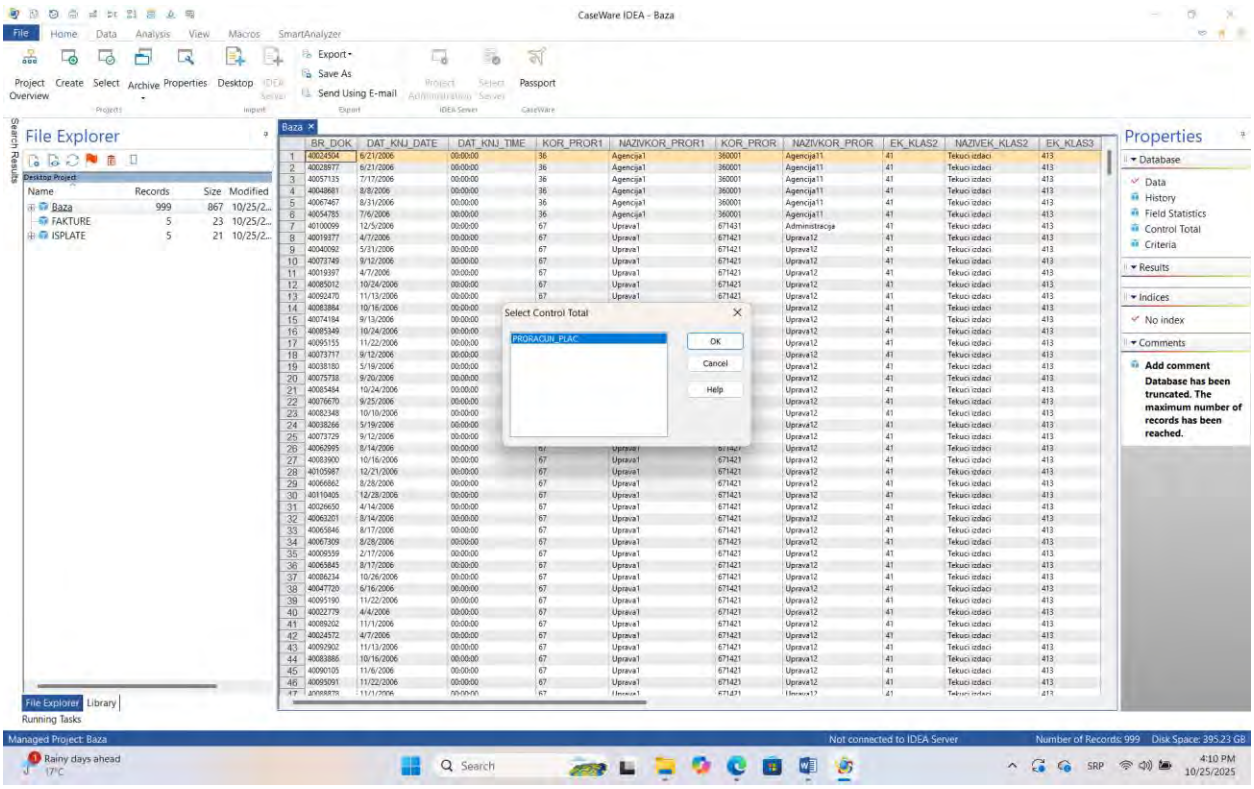


Slika 19. Kartica Field Statistics u Properties prozoru

Funkcija **Control Totals** koristi se za izračunavanje i prikaz kontrolnih zbirova nad numeričkim poljima u bazi podataka. Kontrolni zbir predstavlja ukupnu vrijednost odabranog polja i koristi se za provjeru potpunosti i tačnosti uvezenih podataka. Postupak je sljedeći:

- Otvoriti bazu podataka u **Database Window**.
- U **Properties** prozoru izabrati karticu **Control Totals** (vidi Sliku 20).
- U prozoru koji se otvori kliknuti na polje za izračunavanje kontrolnog zbira.
- IDEA automatski izračunava zbir svih vrijednosti u izabranom polju i prikazuje ga u **Properties** pod **Control Totals**.
- Kontrolni zbirovi se mogu uporediti sa izvorima (npr. glavnom knjigom) radi potvrde da je uvoz podataka izvršen ispravno i u cjelini.
- Izborom novog polja za kontrolni zbir pojavljuje se novi umjesto starog.

Ova funkcija omogućava revizoru da provjeri integritet baze i da se uvjeri da svi relevantni iznosi odgovaraju knjigovodstvenim evidencijama ili drugim kontrolnim izvorima podataka.

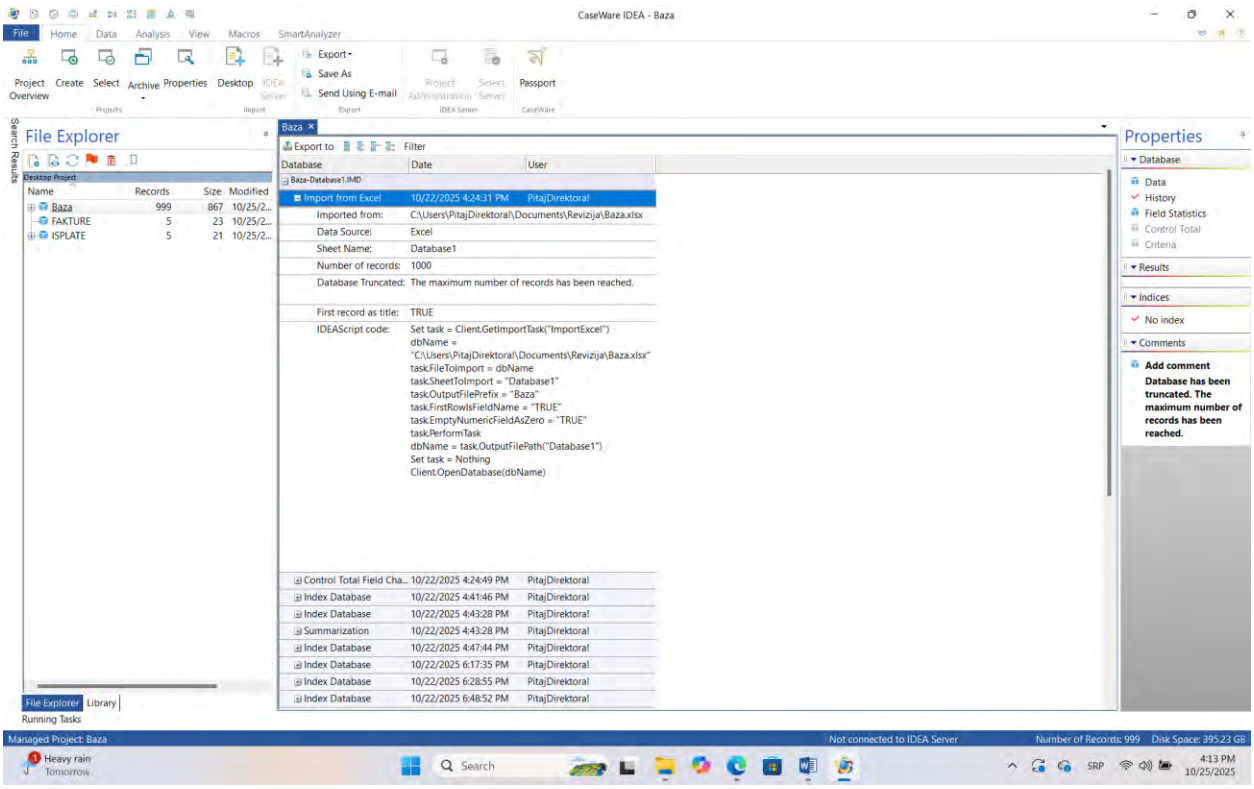


Slika 20. Kartica Control Totals u Properties prozoru

Opcija **History** predstavlja automatski dnevnik svih aktivnosti koje su izvršene nad bazom podataka. IDEA bilježi svaku radnju – od uvoza i formatiranja do primjene analiza i filtriranja – čime se obezbjeđuje potpuni **audit trail** (trag revizije). Postupak je sljedeći:

- Otvoriti bazu podataka u **Database Window**.
- U **Properties** prozoru izabrati karticu **History** (vidi Sliku 21).
- IDEA prikazuje hronološku listu svih izvršenih operacija, uključujući:
  - naziv komande (npr. *Import*, *Extract*, *Summarization*),
  - datum i vrijeme izvršenja,
  - korisnika koji je pokrenuo radnju,
  - opis rezultata (npr. broj zapisa u novoj bazi, primijenjeni uslovi i sl.).
- Svaka zabilježena radnja može se pregledati detaljno klikom na plus sa lijeve strane.
- Klikom na dugme **Export to** moguće je eksportovati istoriju u Word ili PDF radi dokumentovanja revizijskog postupka.
- IDEA automatski čuva istoriju zajedno sa projektom, tako da se sve aktivnosti mogu naknadno pregledati bez dodatnog evidentiranja.

Kartica History ima ključnu ulogu u obezbjeđivanju revizijskog traga, jer omogućava potpunu transparentnost rada i lako dokazivanje izvršenih analiza i transformacija podataka.



Slika 21. Kartica History sa zabilježenim radnjama

7.5. Analiza

Analitičke funkcije IDEA-e (CaseWare IDEA Inc, 2018) čine srž njenog revizijskog značaja. Korisnici mogu primjenjivati različite metode za identifikaciju nepravilnosti, obrazaca i rizika. Najvažnije analize su:

- **Sortiranje** – brzo pronalaženje ekstremnih vrijednosti.
- **Statistika polja**– opisna statistika za svako polje (raspon, prosjek, odstupanja).
- **Ekstrakcija** – pronalaženje zapisa koji ispunjavaju određene uslove.
- **Sumarizacija** – grupisanje i izračunavanje zbirnih pokazatelja po kategorijama (npr. ukupan iznos po dobavljaču).
- **Detekcija praznina i duplikata** – detekcija niza grešaka koje mogu ukazivati na prevare ili greške u unosu.
- **Statističko uzorkovanje** – izdvajanje reprezentativnog uzorka.
- **Benfordova analiza** – test prirodne distribucije prvih cifara radi otkrivanja manipulacija – u velikim skupovima stvarnih podataka manje cifre (npr. 1, 2, 3) pojavljuju se češće kao prva cifra nego veće cifre (npr. 8, 9).
- **Stratifikacija** – klasifikacija podataka u slojeve prema iznosima, što pomaže pri izboru uzorka ili analizi rizika.

- **Spajanje baza** – spajanje ili poređenje podataka iz više izvora, npr. faktura i isplata radi otkrivanja razlika.

Rezultati svake analize mogu se **izvesti** (**Export**) u Excel, PDF ili drugi format i uključiti u revizorsku dokumentaciju.

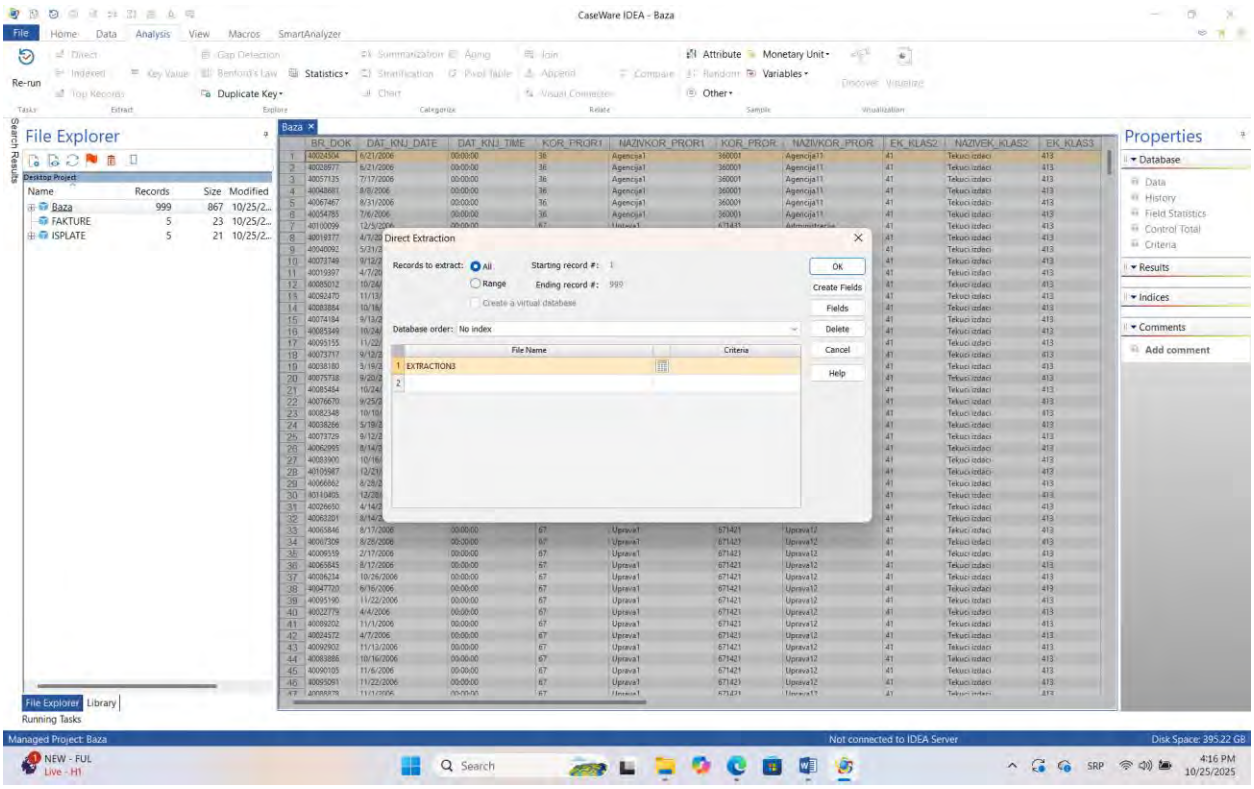
Postupke za **sortiranje** i **statistiku polja** smo već opisali u prethodnoj sekciji.

Ekstrakcija se obavlja pomoću **Extract** funkcije, koja je vidljiva kada se klikne **Analysis** u meniju na vrhu prozora. Funkcija **Extract** koristi se za izdvajanje određenih zapisa iz baze podataka prema definisanim kriterijumima. Na taj način moguće je formirati nove podskupove podataka koji ispunjavaju određene uslove, bez izmjene originalne baze. IDEA nudi više vrsta ekstrakcije, od kojih su najčešće korišćene **Direct** i **Top Records**.

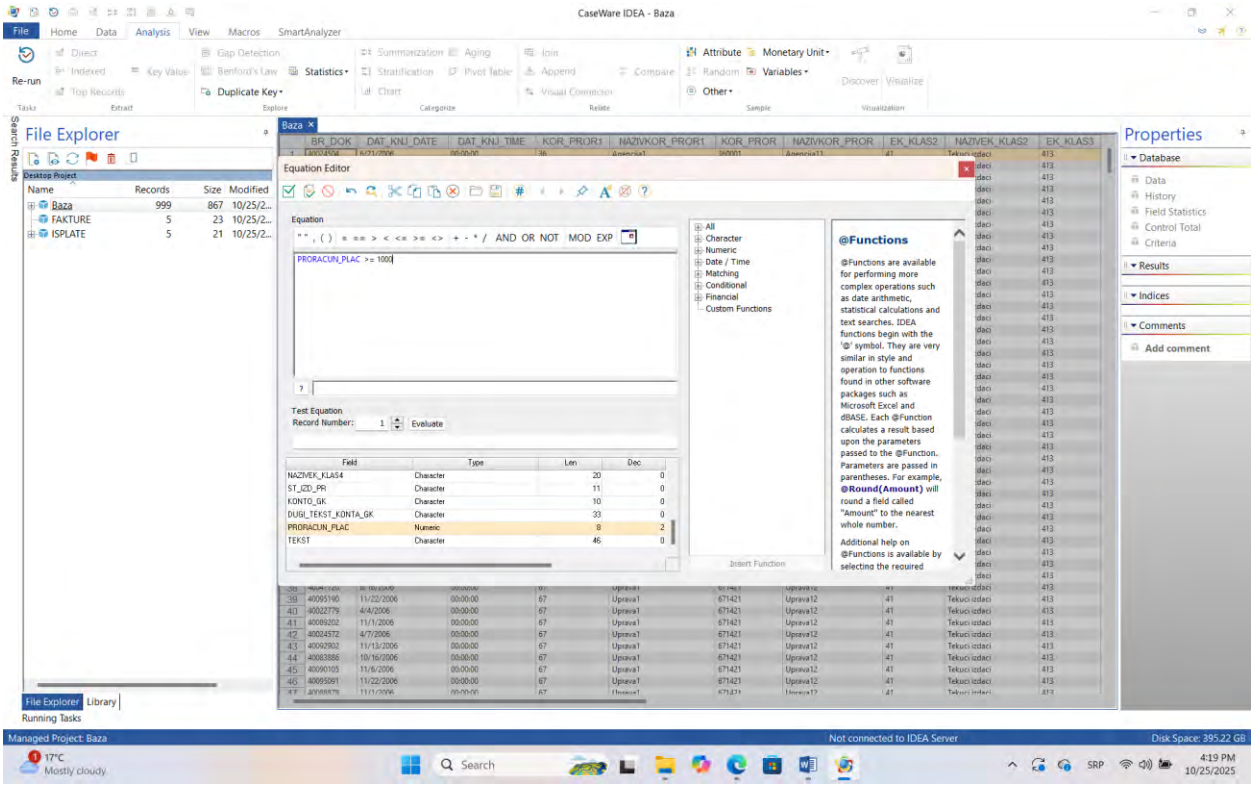
Opcija **Direct** omogućava izdvajanje svih zapisa koji ispunjavaju tačno određene kriterijume, definisane pomoću izraza ili logičkih uslova. Postupak je sljedeći:

- U otvorenoj bazi podataka na kartici **Analysis – Extract** izabrati komandu **Direct** (vidi Sliku 22).
- U otvorenom dijalogu kliknuti na ikonicu digitrona u sredini za definisanje kriterijuma (vidi Sliku 23).
- U dijalogu koji se otvori, u polje **Equation** unijeti uslov po kojem se podaci izdvajaju, npr.:
    - AMOUNT > 10000 – izdvajanje svih transakcija većih od 10.000,
    - REGION = „EU“ – izdvajanje zapisa koji pripadaju određenoj regiji,
    - AMOUNT > 10000 AND REGION = „EU“ – kombinovani uslov.
- Polja, logički operatori i logičke funkcije, koji su vidljivi u dijalogu, se automatski prenose u uslov duplim klikom na njih.
- Datumske vrijednosti se automatski prenose izborom datuma iz kalendara koji je vidljiv u dijalogu.
- Vrijednosti za numerička polja se direktno unose, a za tekstualna polja pod navodnicima.
- Klikom na dugme **Validate (zeleni štrik)** moguće je provjeriti ispravnost izraza.
- U polje **File Name** unijeti naziv nove baze u koju će se izdvojeni zapisi sačuvati.
- Kliknuti **OK** da bi IDEA kreirala novu bazu sa samo onim zapisima koji zadovoljavaju zadate kriterijume.
- Nova baza se pojavljuje u **File Explorer** prozoru (kao podbaza izvorne baze) i može se dalje analizirati nezavisno od izvorne baze.

Direktna ekstrakcija koristi se za fokusirano izdvajanje relevantnih podataka, što omogućava bržu analizu i smanjuje obim baze sa kojom se radi.



Slika 22. Kartica Analysis i odjeljak Extract → Direct

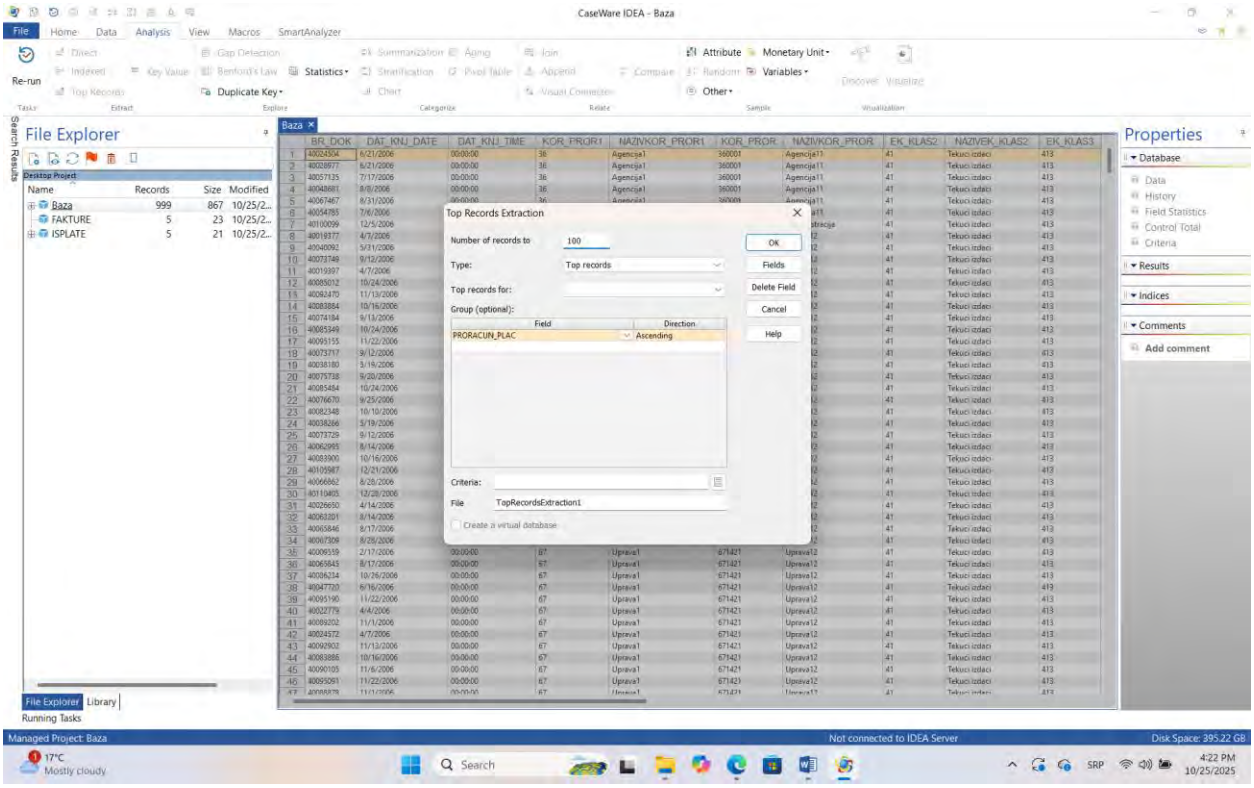


Slika 23. Dijalog za definisanje uslova ekstrakcije (Equation Editor)

Opcija **Top Records** omogućava izdvajanje ograničenog broja prvih zapisa iz baze, prema zadatom kriterijumu sortiranja. Koristi se za analizu najvećih ili najmanjih vrijednosti u određenom polju (npr. najviših iznosa faktura, najvećih isplata ili najstarijih datuma). Postupak je:

- U otvorenoj bazi na kartici **Analysis – Extract** izabrati **Top Records**.
- U dijalogu koji se otvori, izabrati polje po kojem će se vršiti sortiranje (vidi Sliku 24).
- U polju **Type** odabrati:
  - **Top records** – za izdvajanje najvećih vrijednosti,
  - **Bottom records** – za izdvajanje najmanjih vrijednosti.
- U polje **Number of Records** unijeti broj zapisa koji će biti izdvojeni (npr. 10, 50, 100).
- U polje **File** upisati naziv nove baze i kliknuti **OK**.
- IDEA kreira novu bazu koja sadrži samo odabrani broj zapisa sa vrha ili dna liste.
- Nova baza se pojavljuje u **File Explorer** prozoru kao podbaza izvorne baze.

Ova funkcija se često koristi za identifikaciju najvećih transakcija, potencijalno rizičnih iznosa ili kontrolu pravilnosti obrade podataka kod ekstremnih vrijednosti.



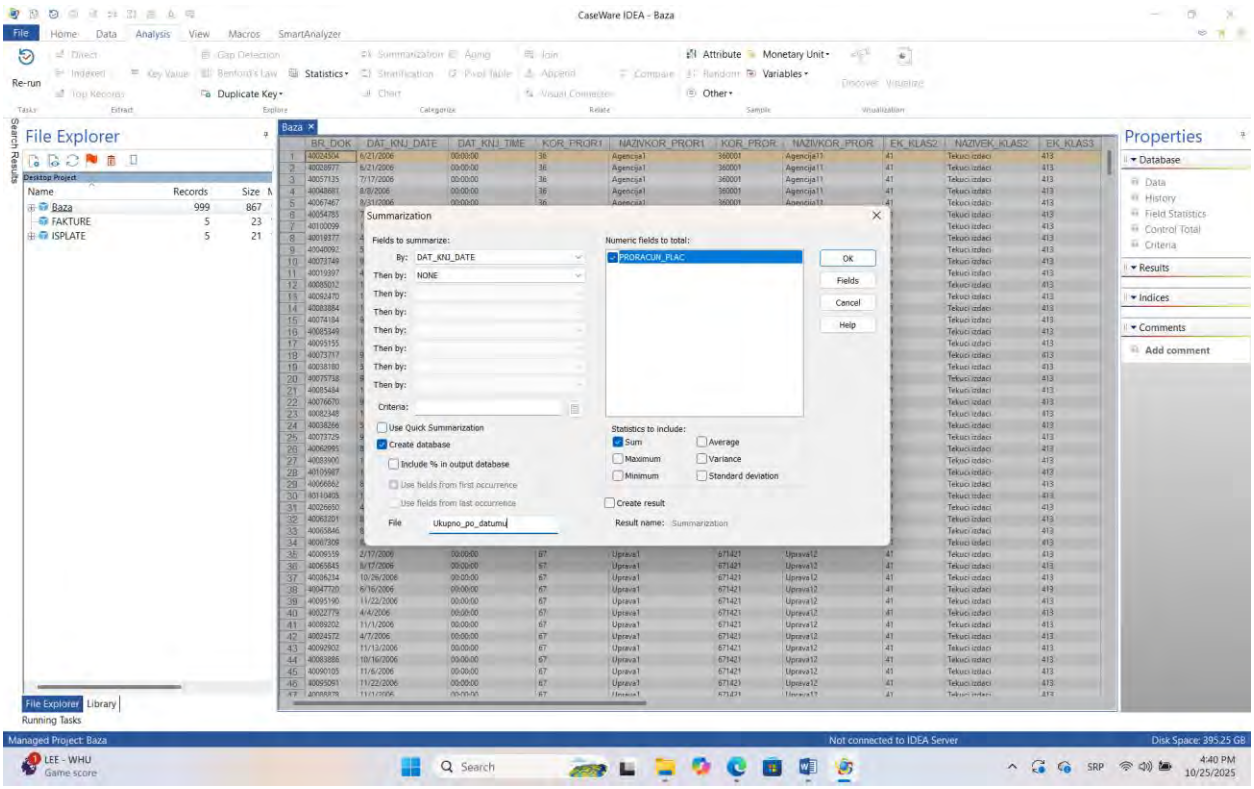
Slika 24. Dijalog Top Records (izdvajanje najvećih vrijednosti)

Sumarizacija se obavlja pomoću **Summarization** opcije u okviru **Categorize** odjeljka **Analysis** kartice. Sumarizacija se koristi za grupisanje podataka prema jednom ili više polja i izračunavanje zbirnih vrijednosti za svaku grupu. Na taj način moguće je brzo dobiti sažete informacije o strukturi podataka, kao što su ukupni iznosi po kupcima, regionima, računima ili datumu. Postupak je:

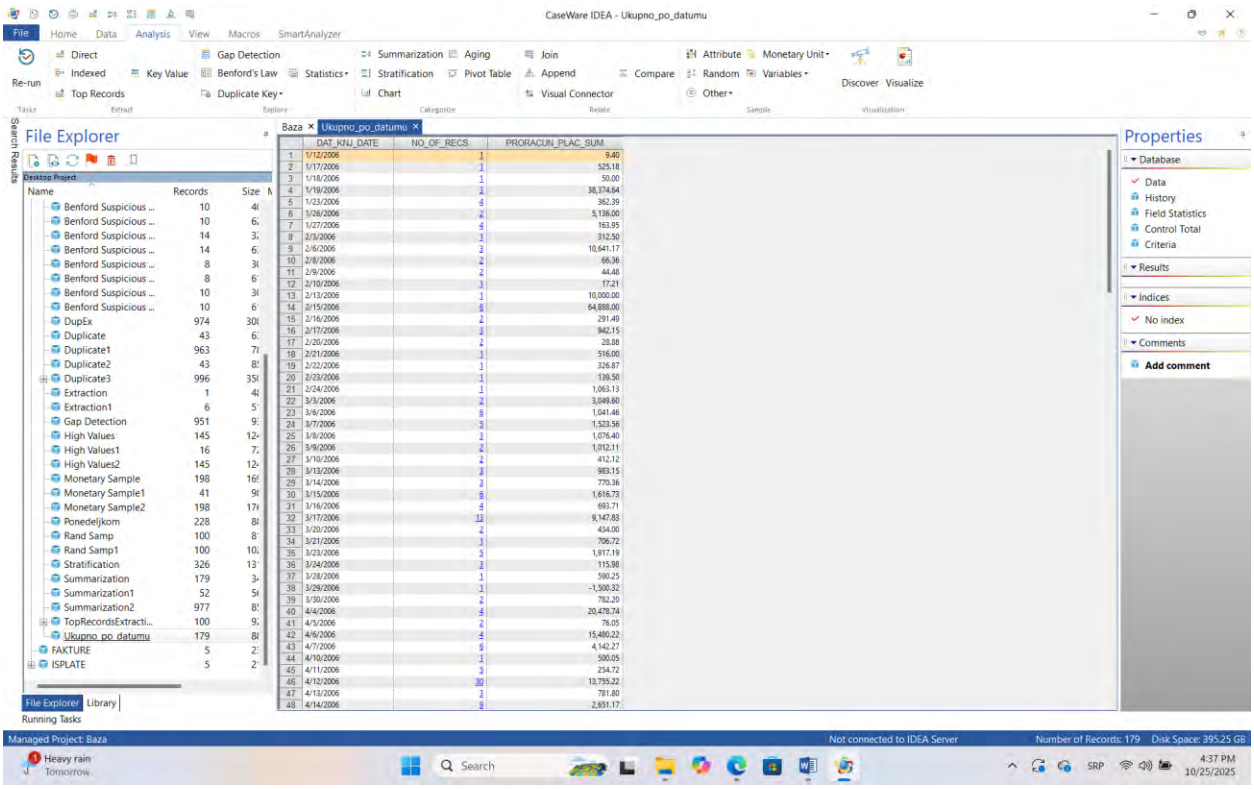
- U otvorenoj bazi podataka na kartici **Analysis – Categorize** izabrati komandu **Summarization**.

- U dijalogu koji se otvori (vidi Sliku 25), u polju **Fields to Summarize** izabrati jedno ili više polja prema kojima će se podaci grupisati (npr. *Customer_ID*, *Region*).
- U dijelu **Numeric Fields to Total** izabrati polje ili više njih čiji će se iznosi sabirati (npr. *Amount*, *Invoice_Value*).
- Po potrebi uključiti dodatne opcije:
  - **Minimum / Maximum** – prikazuje najmanju i najveću vrijednost u okviru grupe
  - **Average** – izračunava prosječnu vrijednost
  - **Standard deviations** – izračunava prosječno odstupanje od sredine.
- U polje **File** unijeti naziv nove baze u kojoj će se sažeti rezultati sačuvati (npr. *Sales_by_Region*).
- Kliknuti **OK** da bi IDEA izvršila sumarizaciju i kreirala novu bazu podataka.
- Rezultati se prikazuju u tabeli koja sadrži po jedan red za svaku grupu i zbirne vrijednosti u odgovarajućim kolonama (vidi Sliku 26).
- Nova baza je vidljiva u **File Explorer** prozoru kao podbaza izvorne baze.

Sumarizacija omogućava pregled koncentracije podataka i brzo otkrivanje neobičnih odstupanja, kao što su izuzetno velike vrijednosti po pojedinim kategorijama ili neuobičajen broj zapisa u određenoj grupi. Ova funkcija je posebno korisna u revizijskoj analizi za provjeru potpunosti i konzistentnosti zbirnih iznosa.



Slika 25. Dijalog Summarization (polja za grupisanje i sabiranje)



Slika 26. Rezultat sumarizacije (tabela sa zbirnim vrijednostima)

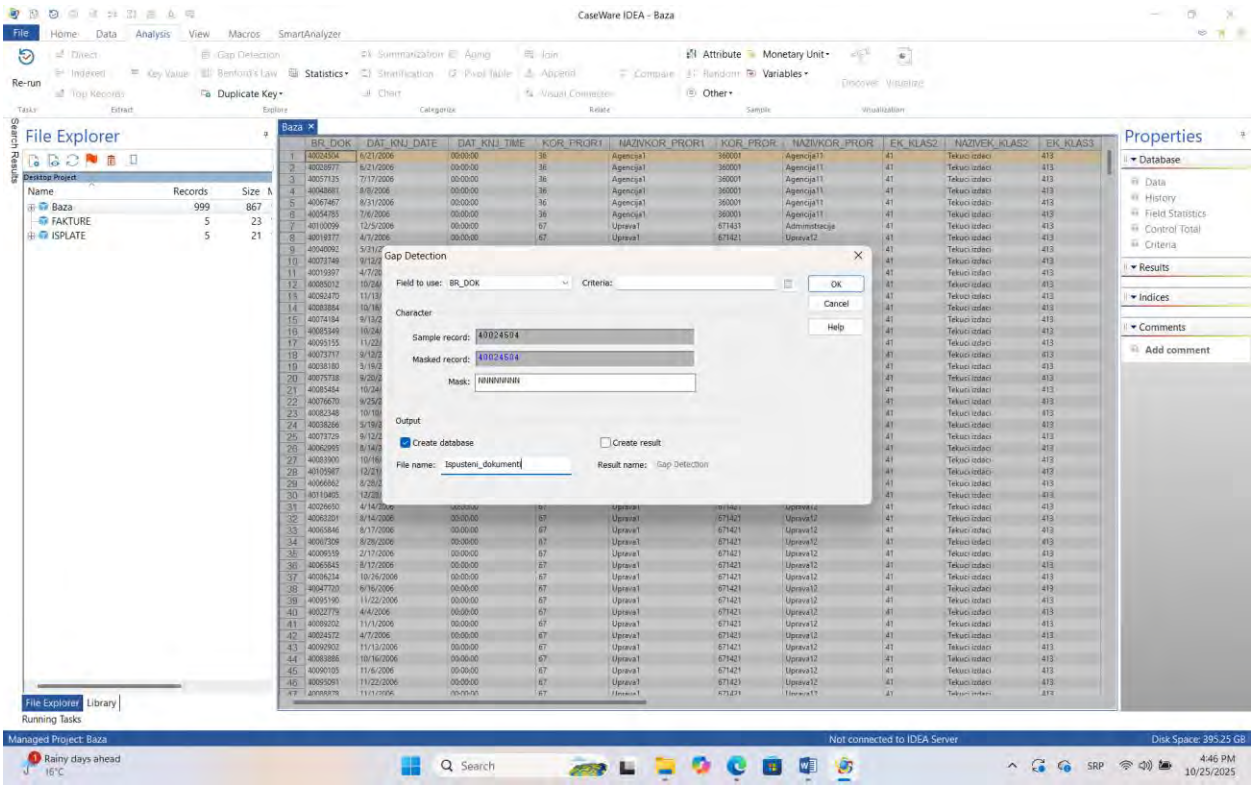
Detekcija praznina se obavlja pomoću opcije **Gap Detection** u okviru **Explore** odjeljka **Analysis** kartice. Koristi se za otkrivanje nedostajućih vrijednosti u nizovima koji bi trebalo da budu kontinuirani – kao što su brojevi faktura, čekova, naloga ili drugih serijskih zapisa. Ova analiza pomaže da se identifikuju mogući propusti, izostavljene transakcije ili nepravilnosti u redosljedu poslovnih događaja. Postupak je sljedeći:

- U otvorenoj bazi podataka na kartici **Analysis – Explore** izabrati komandu **Gap Detection**.
- U dijalogu koji se otvori (vidi Sliku 27), u polju **Field to Use** izabrati polje koje sadrži serijski niz (npr. *Invoice_Number*, *Check_ID*).
- U polje **File name** unijeti naziv nove baze u kojoj će se prikazati rezultati (npr. *Missing_Invoices*) (**Create database** mora biti čekirano).
- Kliknuti **OK**. IDEA kreira novu bazu koja prikazuje sve otkrivene praznine u nizu – tj. gdje nedostaju određene vrijednosti (vidi Sliku 28).
- Nova baza je vidljiva u **File Explorer** prozoru kao podbaza izvorne baze.

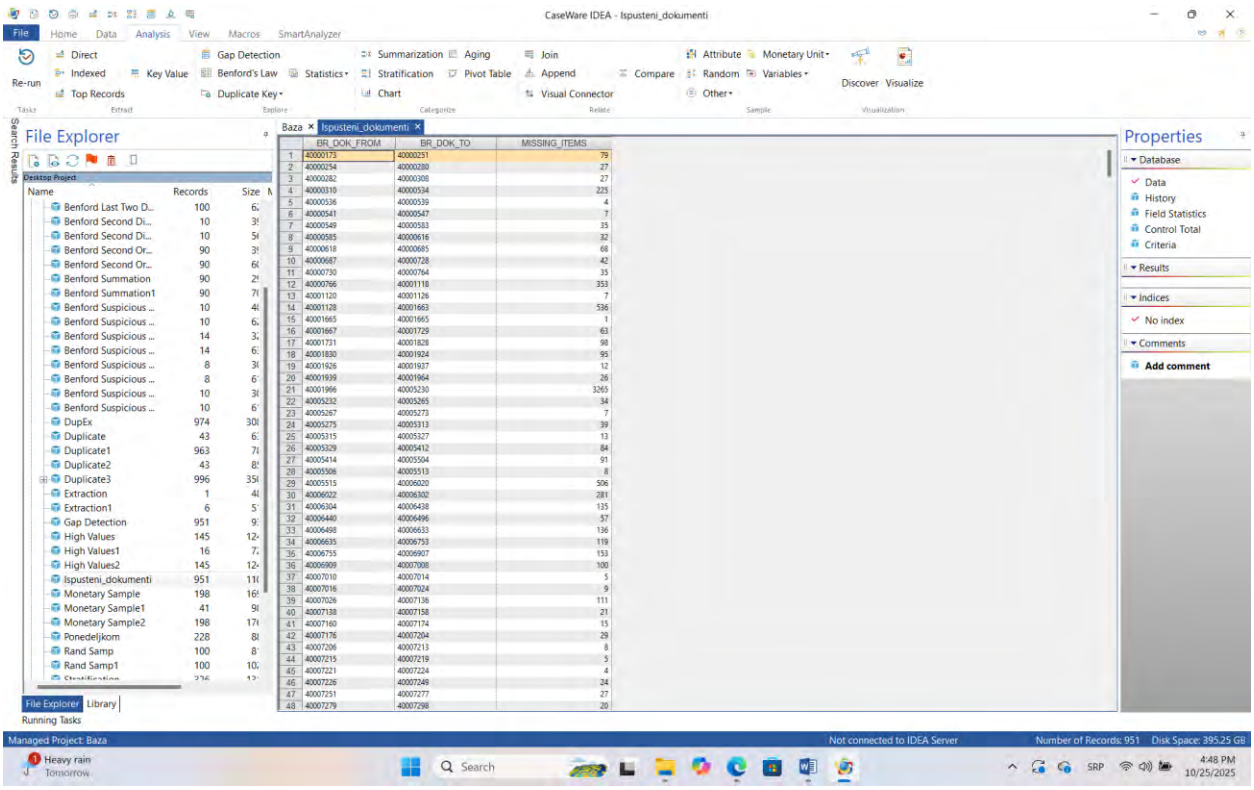
Rezultati analize sadrže tri ključne kolone:

- **From / To** – granice između kojih je pronađena praznina,
- **Missing_Items** – broj izostavljenih vrijednosti u tom rasponu.

Ova funkcija je naročito korisna u revizijskoj praksi za provjeru **potpunosti evidencije** i otkrivanje **neobjašnjenih prekida** u sekvencijalnim zapisima, što može ukazivati na greške u unosu ili namjerno izostavljanje.



Slika 27. Dijalog Gap Detection (izbor polja i naziv baze)



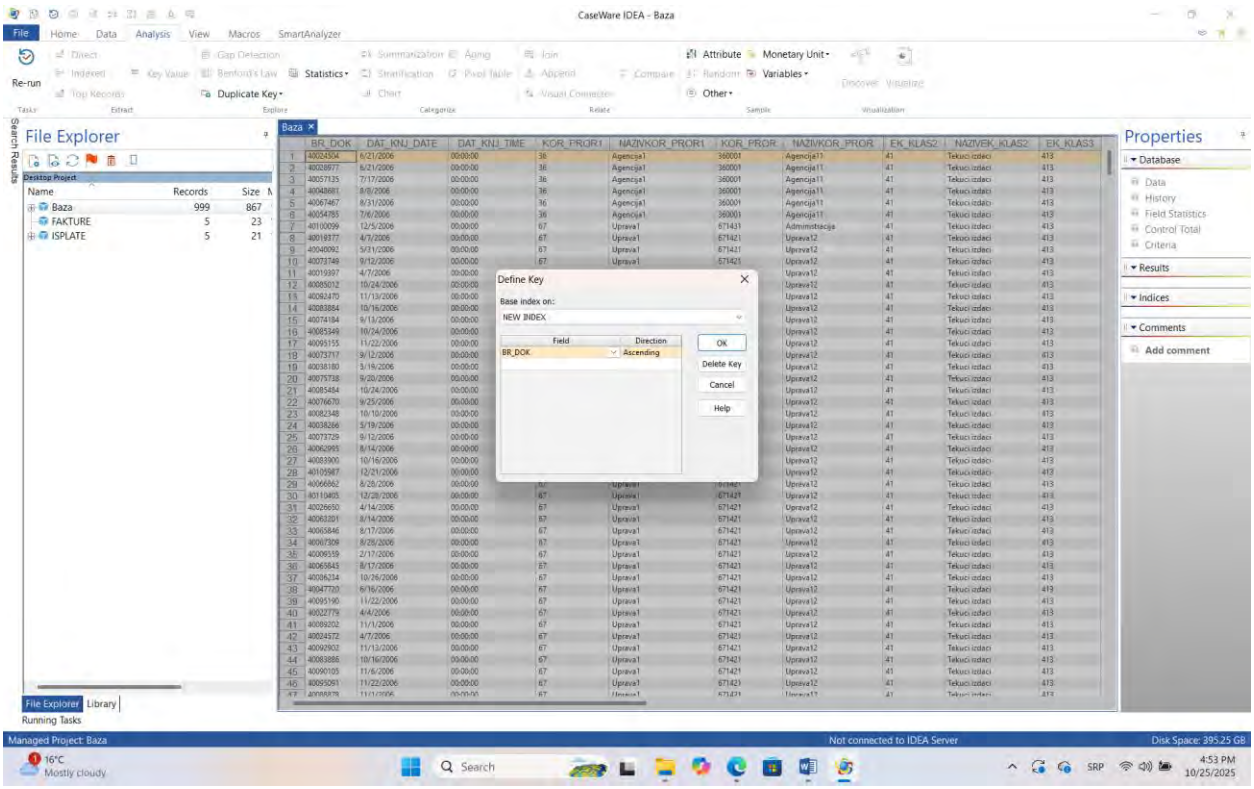
Slika 28. Rezultat detekcije praznina (Missing Items)

Detekcija duplikata se koristi za pronalaženje zapisa koji imaju iste vrijednosti u jednom ili više polja koja bi trebalo da budu jedinstvena. Ova analiza pomaže u otkrivanju duplih faktura, isplata, naloga ili drugih ponovljenih transakcija koje mogu ukazivati na grešku ili potencijalnu zloupotrebu. Postupak se sastoji od sljedećih koraka:

- U otvorenoj bazi podataka na kartici **Analysis – Explore** izabrati komandu **Duplicate Key Detection**.
- U dijalogu koji se otvori, kliknuti na **Key** pa u dijelu **Field** izabrati jedno ili više ključnih polja prema kojima se provjerava jedinstvenost (npr. *Invoice_Number*, *Vendor_ID*, *Date*), a u dijelu **Direction** poredak kojim će rezultat biti prikazan (vidi Sliku 29). Na kraju kliknuti na **OK**.
- U polje **File name** unijeti naziv baze u kojoj će IDEA sačuvati rezultate (npr. *Duplicate_Invoices*).
- Kliknuti **OK**. IDEA kreira novu bazu koja sadrži samo zapise kod kojih su pronađeni duplikati.

U rezultujućoj tabeli prikazuju se polja po kojima je detekcija vršena, uređena u rastućem ili opadajućem redosljedu po prvom polju, pa u okviru njega po drugom itd.

Ova analiza omogućava revizoru da brzo identifikuje sumnjive zapise, kao što su dvostruke isplate istom dobavljaču, ponovljeni brojevi faktura ili duplikati unosa, čime se povećava tačnost i pouzdanost revizijskih nalaza.

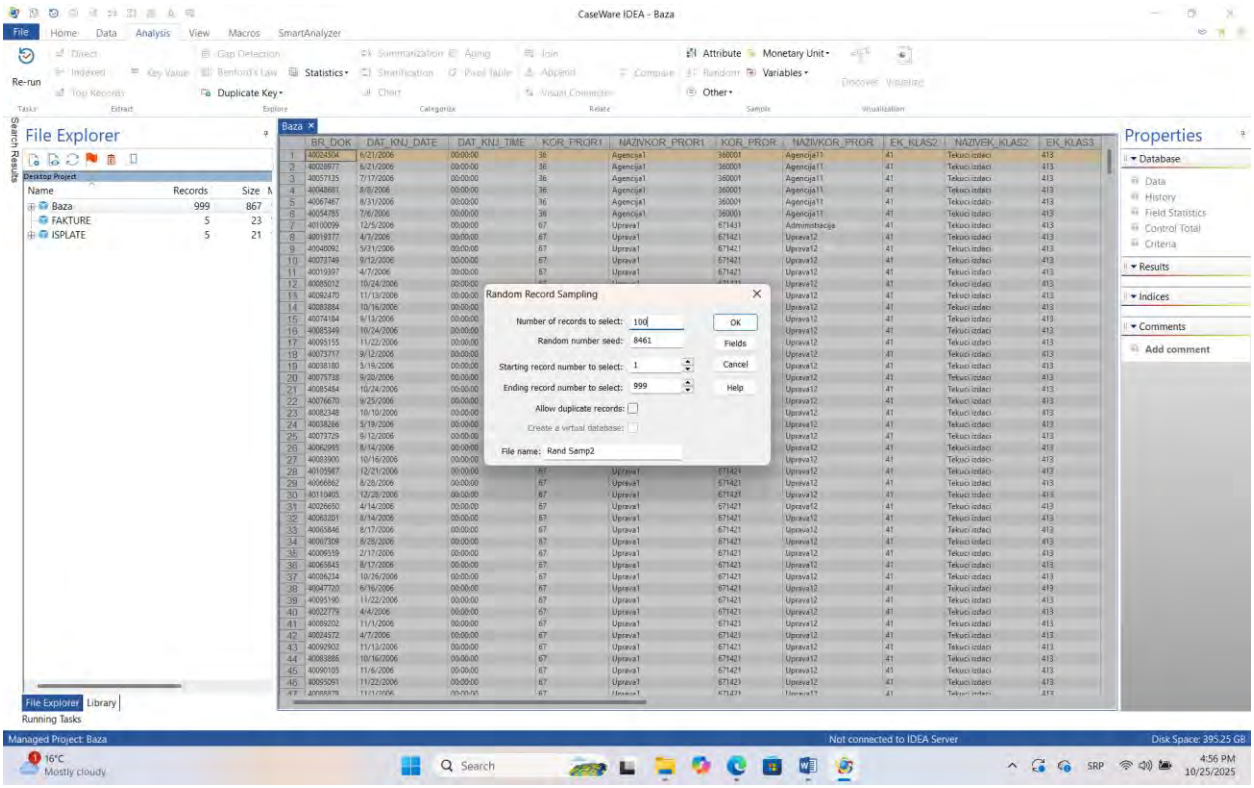


Slika 29. Dijalog Duplicate Key Detection (izbor ključnih polja)

Uzorkovanje se koristi za izdvajanje reprezentativnog uzorka iz velike baze podataka, omogućavajući revizoru da testira manji broj zapisa, a da pritom rezultati budu dovoljno pouzdani za donošenje zaključaka o cjelokupnom skupu podataka. **Slučajno uzorkovanje** omogućava nasumičan izbor zapisa iz baze, bez obzira na njihovu vrijednost. Svaki zapis ima jednaku vjerovatnoću da bude izabran. Postupak je sljedeći:

- U otvorenoj bazi podataka na kartici **Analysis – Sample** izabrati **Random**.
- U dijalogu koji se otvori u polju **Number of records to select** upisati tačan broj zapisa koji treba izdvojiti (npr. 50) (vidi Sliku 30).
- U polje **File name** unijeti naziv nove baze (npr. *Random_Sample*).
- Kliknuti **OK**. IDEA automatski nasumično bira zapise i formira novu bazu koja sadrži samo izabrane stavke.

Ova metoda se koristi kada svi zapisi imaju jednaku važnost, a cilj je dobiti nepristrasan uzorak za testiranje.



Slika 30. Dijalog Sampling (Random)

Spajanje baza kombinuje dvije baze podataka na osnovu zajedničkog polja (ključa). Na taj način mogu se objediniti povezane informacije iz različitih izvora i analizirati u jedinstvenoj tabeli. Takođe, mogu se izdvojiti zapisi koji se pojavljuju samo u prvoj bazi ili zapisi koji se pojavljuju samo u drugoj bazi. Postupak spajanja baza objasnićemo na sljedećem primjeru.

Revizor želi da provjeri da li su sve izvršene isplate povezane sa postojećim fakturama u sistemu. Za tu svrhu koristi funkciju **Join** (na kartici **Analysis – Relate**), koja povezuje dvije baze pomoću zajedničkog polja.

Baze su **FAKTURE** i **ISPLATE**:

Baza: FAKTURE

Broj_fakture	Dobavljač	Datum_fakture	Iznos (€)
F-101	D001	5. 3. 2024.	2.350
F-102	D002	7. 3. 2024.	4.800
F-103	D003	8. 3. 2024.	1.250
F-104	D004	9. 3. 2024.	3.600
F-105	D005	11. 3. 2024.	2.900

Baza: ISPLATE

ID_isplate	Broj_fakture	Datum_isplate	Iznos (€)
P-01	F-101	15. 3. 2024.	2.350
P-02	F-102	17. 3. 2024.	4.800
P-03	F-103	18. 3. 2024.	1.250
P-04	F-104	20. 3. 2024.	3.600
P-05	F-110	21. 3. 2024.	5.000

Vizuelnim uvidom u podatke vidi se da se u bazi **ISPLATE** pojavljuje zapis: **Broj_fakture = F-110**, iznos **5.000 €**, koji **ne postoji** u evidenciji **FAKTURE**. To znači da je izvršena isplata koja **nije povezana ni sa jednom odobrenom fakturom**.

Postupak otkrivanja pomoću funkcije **Join** je sljedeći:

- Aktivira se baza **ISPLATE**
- Na kartici **Analysis** izabere se komanda **Join**.
- U dijalogu koji se otvori izabrati (vidi Sliku 31):
    - **Primary Database:** ISPLATE
    - **Secondary Database:** FAKTURE
- Kliknuti na **Match** i izabrati zajedničko polje **Broj_fakture** za **Primary** i **Secondary**.
- Odabrati **Records with no secondary match**, kako bi IDEA prikazala isplate koje **nemaju odgovarajuće fakture**.
- U polje **File name** unijeti naziv nove baze, npr. *Isplate_bez_fakture*, i kliknuti **OK**.

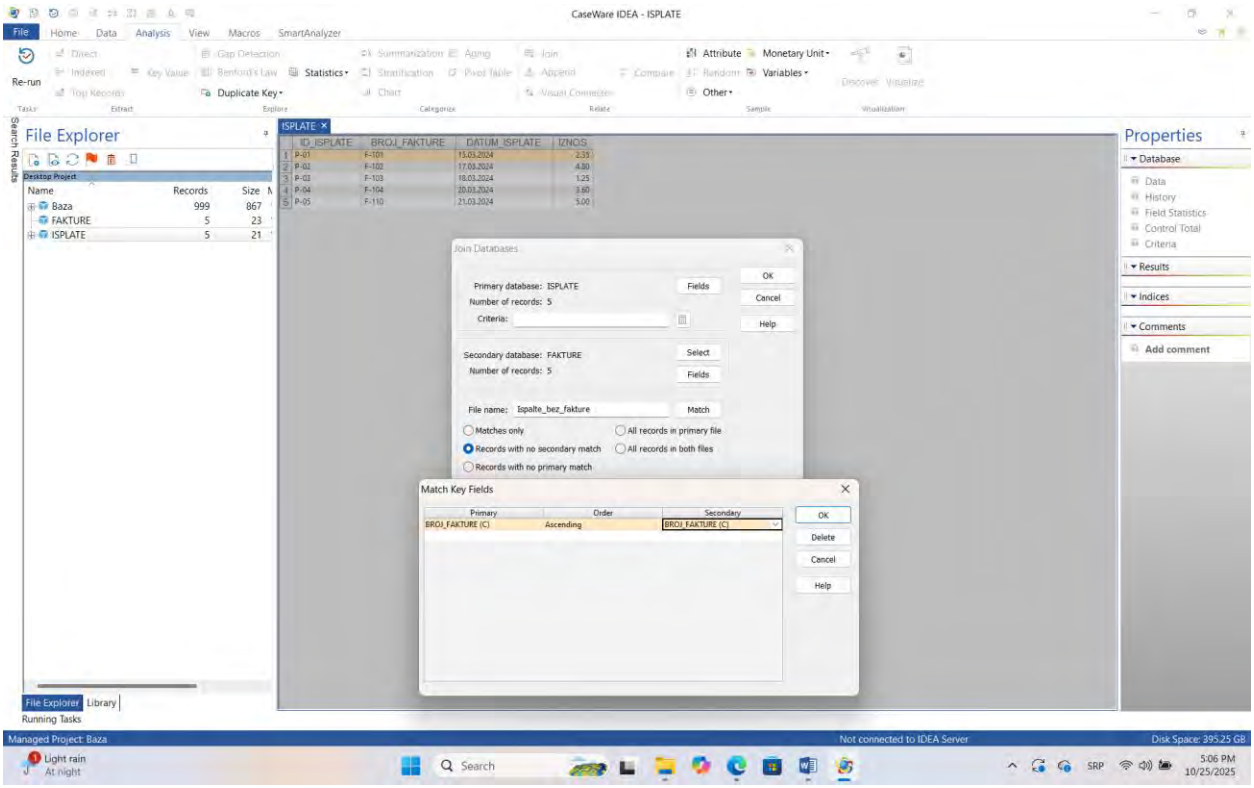
IDEA kreira novu bazu sa zapisima iz **ISPLATE** prikazujući zapise koji nemaju par u **FAKTURE** (vidi Sliku 32):

ID_isplate	Broj_fakture	Datum_isplate	Iznos (€)
P-05	**F-110**	**21. 3. 2024.**	**5.000**

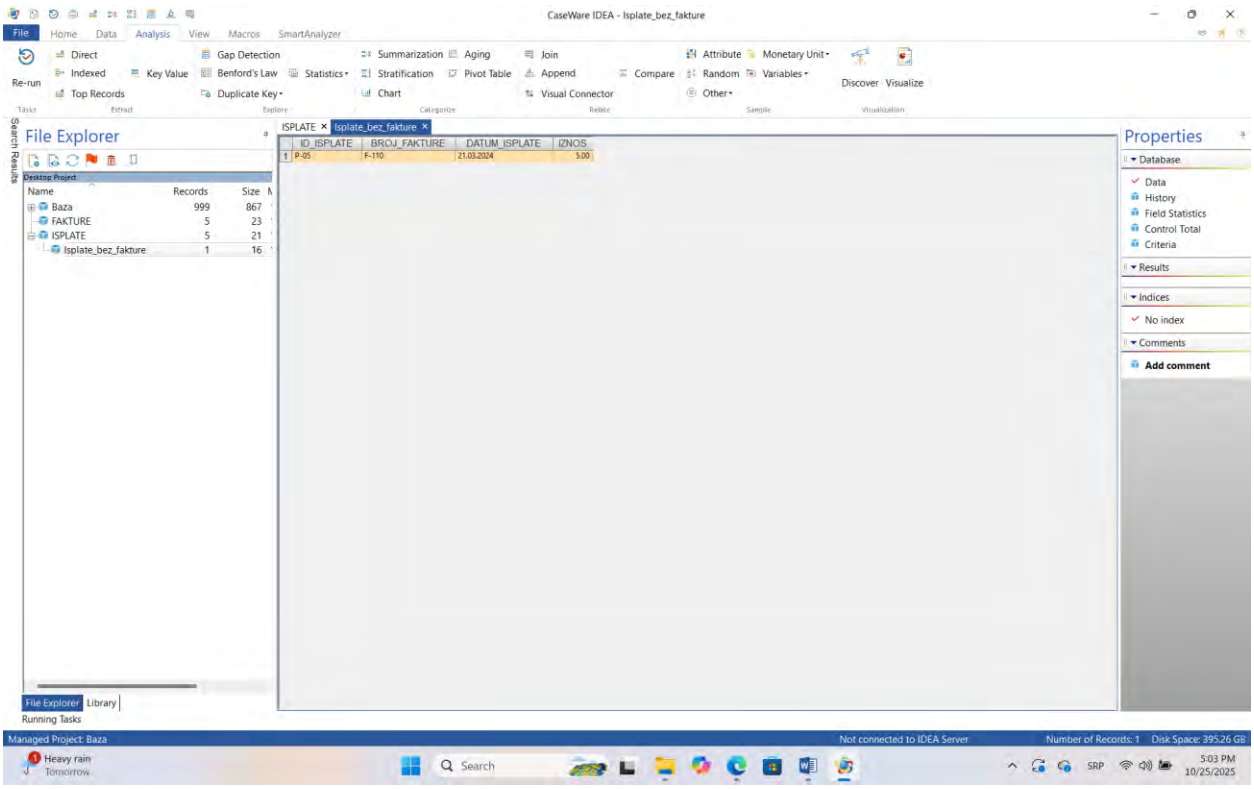
Rezultat jasno pokazuje da je za isplatu **P-05** izvršeno plaćanje bez pripadajuće fakture. Revizor na osnovu ovog nalaza može sprovesti dodatnu provjeru:

- da li je faktura F-110 naknadno proknjižena,
- da li je došlo do greške u unosu broja fakture,
- ili da li postoji osnov sumnje na neovlašćenu isplatu.

Na ovaj način funkcija **Join (Records with no secondary match)** omogućava brzo prepoznavanje **„visećih isplata“**, što je važan korak u otkrivanju nepravilnosti i potvrdi potpunosti finansijskih evidencija.



Slika 31. Dijalog Join (spajanje baza po Broj_fakture)



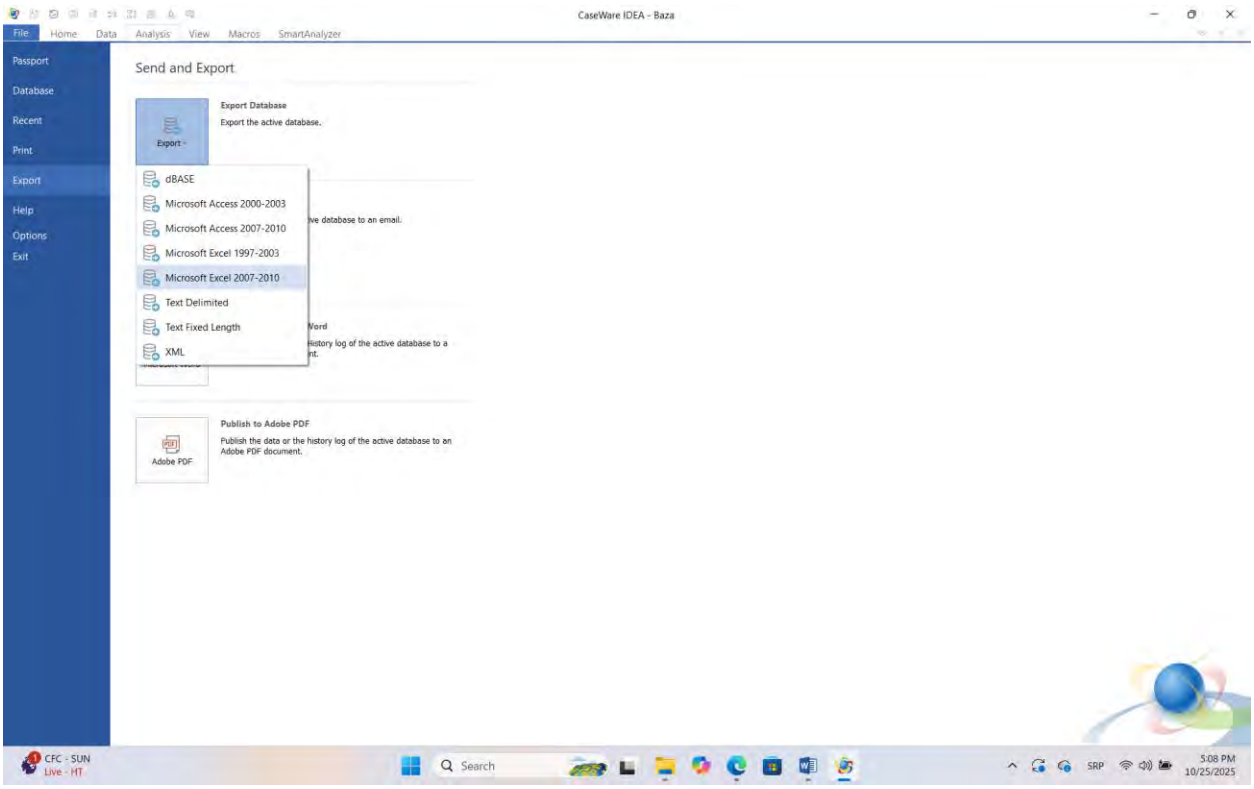
Slika 32. Rezultat Join analize – isplate bez faktura

Export omogućava izvoz rezultata iz IDEA-e u druge formate, kao što su **Excel**, **PDF**, **tekstualni fajl** ili drugi tipovi izvještaja. Ova opcija se najčešće koristi nakon završene analize, kada je potrebno rezultate prezentovati, arhivirati ili uključiti u revizijsku dokumentaciju.

Izvoz u Excel se koristi kada je potrebno dodatno analizirati ili vizualizovati rezultate iz IDEA programa. Postupak je sljedeći:

- Otvoriti bazu podataka čiji se sadržaj želi izvesti (npr. *Isplate_bez_fakture*).
- Na kartici **File** izabrati opciju **Export** (vidi Sliku 33).
- Izabrati opciju **Export Database** i format **Microsoft Excel 2007–2010**.
- U dijalogu koji se otvori:
  - kliknuti **(...)** i izabrati lokaciju za čuvanje fajla
  - unijeti ime fajla (npr. *Rezultati_kontrole_isplata*)
  - kliknuti **Save**
- Kliknuti **OK**. IDEA kreira Excel datoteku koja sadrži sve podatke iz aktivne baze.

Izvezeni Excel fajl zadržava strukturu kolona, formate i nazive polja kao u IDEA-i, čime je spreman za dalje obrađivanje ili slanje revizorskom timu.

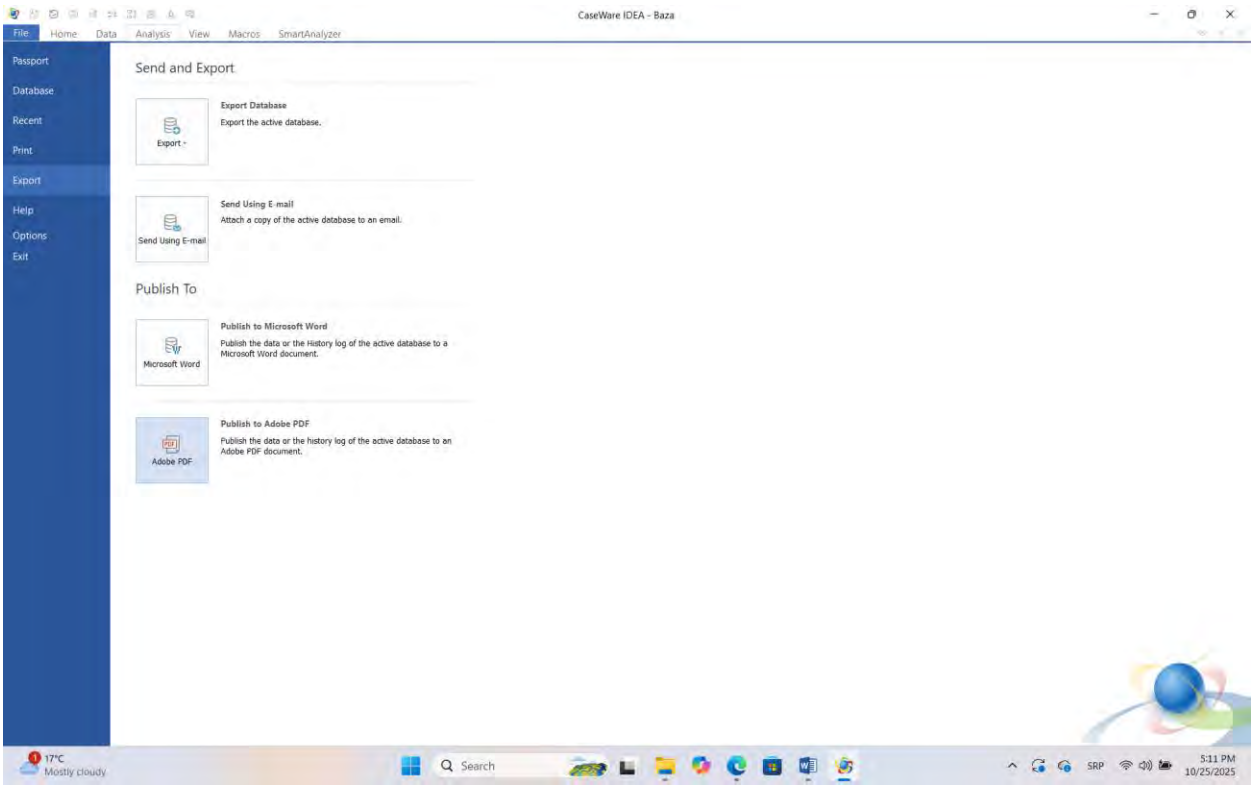


Slika 33. Export u Excel (dijalog za izbor formata i lokacije)

Izvoz u PDF se koristi kada je potrebno sačuvati rezultate u nepromjenljivom formatu pogodnom za arhiviranje i priložiti ih uz revizijski izvještaj. Postupak je:

- Otvoriti bazu sa rezultatima analize.
- Na kartici **File** izabrati **Export**.
- Izabrati opciju **Publish to Adobe PDF** (vidi Sliku 33).
- U prozoru koji se otvori izabrati lokaciju dokumenta, upisati naziv i kliknuti **Save**.
- IDEA generiše PDF dokument koji vjerno prikazuje tabelu sa svim prikazanim rezultatima.

Izvoz podataka omogućava revizoru da jednostavno dokumentuje nalaze, dijeli rezultate sa drugim učesnicima u reviziji i obezbijedi trag o sprovedenim analizama u formatu pogodnom za izvještavanje.



Slika 34. Export u PDF (dijalog Publish to Adobe PDF)

Literatura

1. AIIM. (2021). What is an electronic document management system (EDMS)? Association for Information and Image Management. https://www.aiim.org/What-is-an-EDMS
2. Balkan Insight. (n. d.). E-Governance solutions in the Western Balkans. Retrieved October 19, 2025, from https://balkaninsight.com/e-governance-solutions-in-the-western-balkans/
3. Berners-Lee, T., & Fischetti, M. (2001). Weaving the Web: The original design and ultimate destiny of the World Wide Web. HarperCollins.
4. Braun, R. L., & Davis, H. E. (2003). Computer-assisted audit tools and techniques: Analysis and perspectives. Managerial Auditing Journal, 18(9), 725–731.
5. Business Insider. (2023). China's Ministry of Public Security launches blockchain-based real-name decentralized identifier system. Markets Insider. https://markets.businessinsider.com/news/currencies/chinas-ministry-of-public-security-launches-blockchain-based-real-name-decentralized-identifier-system-1032891627
6. Buyya, R., & Vahid Dastjerdi, A. (Eds.). (2016). Internet of things: Principles and paradigms. Morgan Kaufmann.
7. CaseWare IDEA Inc. (2018). IDEA tutorial (Version 10.4) [PDF file]. https://ezto.mheducation.com/extMedia/bne/Messier_11e/IDEA_Tutorial_10.4.pdf
8. Digi International. (2025). IoT smart city applications. Digi.com. https://www.digi.com/blog/post/iot-smart-city-applications
9. e-Governance Academy (2025). Podcast 🎧 & blog: Training digital safety through cyber resilience in Montenegro. e-Governance Academy. Retrieved October 19, 2025, from https://ega.ee/podcast-blog-training-digital-safety-through-cyber-resilience-montenegro/
10. Erl, T., Puttini, R., & Mahmood, Z. (2013). Cloud computing: Concepts, technology & architecture. Prentice Hall.
11. European Commission. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. Retrieved October 19, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
12. European External Action Service. (2019). Digital governance to accelerate development in Montenegro. https://www.eeas.europa.eu/delegations/montenegro/digital-governance-accelerate-development_en
13. IAASB. (2018). ISA 505 – External Confirmations. International Auditing and Assurance Standards Board. https://www.icab.org.bd/icabadmin/uploads/ckeditor/22442018-IAASB-Handbook-Volume-1.pdf
14. INTOSAI. (2016). ISSAI 5300 – Guidelines on IT Audit. International Organization of Supreme Audit Institutions.
15. ISACA. (2021). COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association.

16. ISO. (2016). ISO 15489-1:2016 – Information and documentation – Records management – Part 1: Concepts and principles. International Organization for Standardization.
17. ISO/IEC. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO. https://www.iso.org/standard/27001
18. Kašćelan, Lj. (2016). Informacione tehnologije za podršku poslovnom odlučivanju. Univerzitet Crne Gore
19. Konica Minolta. (2020). Digital agriculture: How Dutch farmers use precision farming for floriculture. Konica Minolta EU. https://www.konicaminolta.eu/eu-en/rethink-work-blog/business/digital-agriculture-how-dutch-farmers-use-precision-farming-for-floriculture
20. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.
21. Lambert, J. (2015). Microsoft PowerPoint 2016 Step by Step. Microsoft Press. https://ptgmedia.pearsoncmg.com/images/9780735697799/samplepages/9780735697799.pdf
22. Lambert, J. (2016). Microsoft Outlook 2016 Step by Step. Microsoft Press. https://ptgmedia.pearsoncmg.com/images/9780735697782/samplepages/9780735697782.pdf
23. Lambert, J., & Frye, C. (2022). Microsoft Excel Step by Step (Office 2021 and Microsoft 365) [PDF]. Pearson Education. https://ptgmedia.pearsoncmg.com/images/9780137564279/samplepages/9780137564279_Sample.pdf
24. Laudon, K. C., & Laudon, J. P. (2021). Management Information Systems: Managing the Digital Firm (17th ed.). Pearson.
25. Marz, N., & Warren, J. (2015). Big data: Principles and best practices of scalable real-time data systems. Manning Publications.
26. Ministarstvo javne uprave Crne Gore. (2022). *Strategija digitalne transformacije Crne Gore 2022–2026.* Podgorica: Ministarstvo javne uprave. https://www.zzzcg.me/wp-content/uploads/2025/08/strategija-digitalne-transformacije-sa-ap-1.pdf
27. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press.
28. Nazzaro, M. (2025). Generative AI use is 'escalating rapidly' in federal agencies, GAO finds. FedScoop. https://fedscoop.com/generative-artificial-intelligence-use-federal-government-watchdog
29. O'Brien, J. A., & Marakas, G. M. (2011). Management information systems (10th ed.). McGraw-Hill/Irwin.
30. OECD. (2023). *Government at a glance 2023.* OECD Publishing. https://www.oecd.org/governance/government-at-a-glance-22214399.htm
31. Open Government Partnership. (2022). Montenegro: Commitments – e-participation portal. https://www.opengovpartnership.org/members/montenegro/commitments/ME0064
32. Rainer, K., & Turban E. (2009). Uvod u informacione sisteme. DATASTATUS

33. Salesforce. (2025). AI in government: Top use cases in the public sector. Salesforce. https://www.salesforce.com/government/ai
34. The Motley Fool. (2025). What is blockchain technology? https://www.fool.com/terms/b/blockchain/
35. Times of India. (2024). Tambaram to Tindivanam NH to be monitored by IoT, 1st in TN. The Times of India. https://timesofindia.indiatimes.com/city/chennai/tambaram-to-tindivanam-nh-to-be-monitored-by-iot-1st-in-tn/articleshow/122304540.cms
36. Times of India. (2025). Dubai unveils Dubai Live, an AI-powered command hub to digitally govern the city in real time. The Times of India. https://timesofindia.indiatimes.com/world/middle-east/dubai-unveils-dubai-live-an-ai-powered-command-hub-to-digitally-govern-the-city-in-real-time/articleshow/124549282.cms
37. Times of India. (2025). Evidence, exam papers transfer to get fool-proof with AI, IoT system. The Times of India. https://timesofindia.indiatimes.com/city/nagpur/evidence-exam-papers-transfer-to-get-fool-proof-with-ai-iot-system/articleshow/124642152.cms
38. Times of India. (2025). TN to share govt data for AI training: PTR. The Times of India. https://timesofindia.indiatimes.com/city/chennai/tn-to-share-govt-data-for-ai-training-ptr/articleshow/124490072.cms
39. Times of India. (2025). Using digital land records, blockchain: State aims to be free of disputes, Rajan. The Times of India. https://timesofindia.indiatimes.com/city/kochi/using-digital-land-records-blockchain-state-aims-to-be-free-of-disputes-rajan/articleshow/124640577.cms
40. Turner Lee N. and Wnag J. (2025). Governments are turning to blockchain for public good. Here's how. Brookings Institution. https://www.brookings.edu/articles/governments-are-turning-to-blockchain-for-public-good-heres-how
41. UK Government. (2025). New Google partnership will help rid taxpayer of 'ball and chain' legacy tech and aim to upskill 100,000 civil servants in tech and AI. https://www.gov.uk/government/news/new-google-partnership-will-help-rid-taxpayer-of-ball-and-chain-legacy-tech-and-aim-to-upskill-100000-civil-servants-in-tech-and-ai
42. UN DESA. (2024). United Nations E-Government Survey 2024: Accelerating digital transformation for sustainable development. United Nations. https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024
43. University of Nottingham. (2017). Microsoft Word 2016 essentials [PDF]. https://training.nottingham.ac.uk/Public/O2016/WordEssentials.pdf
44. WGITA-IDI. (2022). WGITA – IDI handbook on IT audit for supreme audit institutions.
45. Wheaton Public Library. (n.d.). Introduction to Microsoft Word 2021 [PDF]. Wheaton Public Library. https://www.wheatonlibrary.org/media/document/244
46. Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (7th ed.). Cengage Learning.
47. Yoon, K., Hoogduin, L., & Zhang, L. (2015). Big Data as Complementary Audit Evidence. Accounting Horizons, 29(2), 431–438.
48. Zakon o zaštiti podataka o ličnosti, *Službeni list Crne Gore*, br. 77/24 (2024).

ISBN 978-9940-752-10-1

