

## TRENDOVI SAVREMENOG POSLOVANJA U INFORMACIONIM TEHNOLOGIJAMA

Almedina Hatarić, MA, email: [almedina\\_tr@hotmail.com](mailto:almedina_tr@hotmail.com)

Imran Kasumović, email: [imran.kasumovic@gmail.com](mailto:imran.kasumovic@gmail.com)

Dženita Muratagić, email: [dzeni.muratagic96@gmail.com](mailto:dzeni.muratagic96@gmail.com)

Internacionalni univerzitet Travnik u Travniku, Bosna i Hercegovina

**Sažetak :** Kako 'staro' i već postojeće prilagoditi informacijskoj tehnologiji savremenog poslovanja? S razvojem nove tehnologije razvijaju se i inovativni oblici menadžmenta koji će kompetentno upravljati tom tehnologijom i nadograđivati je. Za tehnologiju je bitno da poveća učinkovitost ljudskog rada i komunikacije. Integracija IT i poslovne organizacije može bit vrlo kompleksna. Formiranjem teorije koja izučava koordinaciju ova dva elemenata, stvara se temelj za njihovo efikasnije i jednostavnije realiziranje. Menadžment tehnologija u poslovnom sistemu isprepletena je operativnim i strateškim barijerama, stoga je potrebno razmotriti poslovne aktivnosti i menadžment odluke koje je potrebno promijeniti da bi se intenzivnim promjenama, barijere ka efektivnom menadžmentu savladale. Načini ostvarivanja konkurentne strategije na globalnom tržištu, mijenjaju se tako što se prilagođavaju inovativnoj tehnologiji. Svi novi oblici koji imaju dramatičan utjecaj na ekonomiju, stvorili su ozračje nove ekonomije. Vrhovni menadžment mora prevladati i prilagoditi poslovni sistem novoj ekonomiji, i tako sofisticirati svoj tradicionalno orijentisan poslovni sistem u moderan.

**Ključne riječi:** poslovanje, informacione tehnologije, menadžment, ekonomija

## MODERN BUSNISS TRENDS IN INFORMATION TECHNOLOGY

**Abstract :** How to adapt 'old' and already existing to the information technology of modern business? With the development of a new technology, innovative management forms are being developed that will be competent to manage and upgrade this technology. For technology it is important to increase the efficiency of human work and communication. Integration of IT and business organizations can be very complex. By forming a theory that studies the coordination of these two elements, it creates the basis for their more efficient and simpler realization. Technology management in the business system is interwoven with operational and strategic barriers, so it is necessary to consider business activities and management decisions that need to be changed in order to by using intense changes overcome barriers that lead to effective management. The ways to achieve a competitive strategy on a global market are changing by adapting to innovative technology. All new forms that have a dramatic impact on the economy have created an atmosphere of a new economy. Supreme management must overcome and adapt the business system to a new economy, and so sophisticate its traditionally oriented business system into a modern one.

**Key words:** business, information technology, management, economy

### UVOD

Informacione tehnologije (IT) imaju fundamentalan uticaj na moderno društvo i zato se, ne bez razloga, kaže da mi živimo u informatičkom dobu. Načini razmjene i prenosa, kao i količina najrazličitijih informacija danas su veći nego ikad prije u historiji. Informacione tehnologije su danas sastavni dio života u takvoj mjeri da je praktično nezamislivo funkcionisanje bilo kojeg dijela naše egzistencije bez njih. Poslovanje, komunikacije pa i svakodnevni život se oslanjaju na pogodnosti koje nude različite oblasti korištenja računara i odgovarajućih tehnologija. Razvoj računara i programa, a u isto vrijeme sve složeniji zahtjevi od strane krajnjih korisnika računarskih tehnologija, usloveli su pojavu velikog broja različitih

rješenja namijenjenih poslovnoj primjeni. Osnovni cilj ovih vrlo različitih rješenja je unaprjeđenje poslovanja.

Razvoj konkurencije i slaba globalna ekonomija izazivaju potrebu da se analizira proces poslovanja - što uključuje strukturu organizacije i kadrove. Cilj je da se postigne više sa manje vremena i sa manje ljudi. Ono što očekujemo da postignemo je: povećanje produktivnosti, bolju podršku kupcima i kraće vrijeme do tržišta, odnosno - prednost na tržištu. Međutim, da bi smo ostvarili ovakve ciljeve, potrebno je da: uvedemo ravniju upravljačku strukturu i decentralizujemo donošenje odluka. Naravno, onima koji odlučuju je potrebno na vrijeme dostaviti tačne informacije.

Upotreba informacionih tehnologija ima sve veću upotrebu u formiranju novih proizvoda i usluga. Njena glavna uloga je u mijenjanju poslovnih odnosa, kao i poboljšanju poslovnih aktivnosti unutar preduzeća. Novi oblici informacionih usluga (elektronsko naručivanje, kupovanje na daljinu, itd.) omogućavaju provođenje kvalitetne poslovne politike preduzeća. Naravno, ove tehnologije kod nas polako počinju da preuzimaju bitnu ulogu u komunikaciji na raleciji proizvođač - kupac. Na taj način, dosadašnji „klasični” proizvođači postaju multimedijalni predstavnici informacija koristeći se Internetom ili sopstvenom komercijalnom bazom podataka. Mora se imati u vidu da informacione tehnologije imaju niz prednosti koje se ogledaju u:

- modernizaciji poslovnih aktivnosti uz smanjenje broja zaposlenih,
- boljem finansijskom poslovanju preduzeća,
- racionalnom korištenju kapaciteta, resursa i energije,
- kvalitetnoj distribuciji materijala, roba i usluga

Ovo sve utiče na poboljšanje položaja preduzeća u poslovanju. Informacione tehnologije bitno mijenjaju konkurentne izgleda svih poslovnih procesa tokom procesa proizvodnje, ali i u procesu pružanja usluga preduzeća. One organizacije koje ne znaju šta bi započele sa svojim podacima, koje nisu u stanju da izveduiole ozbiljnije statističke analize ili simulacije, mogu čak i da budu kratkoročno veoma uspješne, ali neće nikada uvidjeti stratešku koristi od informacione tehnologije.

## **1. POSTOJEĆA PRIMJENA IT U POSLOVNIM AKTIVNOSTIMA**

Informaciona mreža pokriva danas kompletnu zemaljsku kuglu, ulazi u svaki dom, svaku fabriku i društvenu ustanovu, povezuje kopnena vozila, avione, brodove i svakog pojedinca. Istovremeno, kompjuteri se nalaze jednako tako u velikim bankarskim sistemima, industrijskim kompleksima i upravljanju saobraćajem kao i u mašinama za pranje rublja, automobilima i dečijim igračkama. Pet glavnih područja u kojima je informaciona tehnologija u potpunosti promijenila dotadašnji život rada su:

1. Informaciona tehnologija kao zamjena za kalkulator (Excel)
2. Informaciona tehnologija kao zamjena za pisaću mašinu (Word)
3. Informaciona tehnologija kao zamjena za arhivu (baze podataka)
4. Informaciona tehnologija kao zamjena za televizor (grafika i multimedija)
5. Informaciona tehnologija kao zamjena za katalog (WWW).

U današnje vrijeme se najčešće poslovni podaci obrađuju na računaru, ali su se zadržali stari načini razmene poslovnih informacija i dokumenata u papirnom formatu. Ako bi se

moгуćnosti postojećih računara i telekomunikacija iskoristile na pravi način mogle bi umnogome da unaprijede poslovanje istovremeno smanjujući troškove, pružajući bolje usluge i smanjile bi se greške do kojih dolazi u radu na klasičan način.

Uticaj informacionih tehnologija na uspješnost poslovanja ogleda se preko kvalitetnog informisanja, kontrole, planiranja, sve do upravljanja i odlučivanja. Važno je istaći dvije vrste uticaja informacione tehnologije na kvalitet poslovanja preduzeća i to:

- Neposredni i lako mjerljivi uticaji - neposredni uticaji obuhvataju uštede u resursima (rad, materijal, energija), uštede u vremenu ili pojednostavljenje i racionalizacija nekog poslovnog procesa u preduzeću. Neposredni uticaji se iskazuju brojkama
- Posredni i teško mjerljivi učinci - posredni učinci su važniji, ali teže ih je pratiti, odnosno izmeriti

Nove tehnologije su temelj za nove proizvode, omogućavaju bolju vezu sa kupcima. Upotreba informacionih tehnologija ima sve veću upotrebu u formiranju novih proizvoda i usluga. Njena glavna uloga je u mijenjanju poslovnih odnosa, kao i poboljšanju poslovnih aktivnosti unutar preduzeća. Novi oblici informacionih usluga (elektronsko naručivanje, kupovanje na daljinu, itd.) omogućavaju sprovođenje kvalitetne poslovne politike preduzeća. Naravno, ove tehnologije kod nas polako počinju da preuzimaju bitnu ulogu u komunikaciji na raleciji proizvođač – kupac. Na taj način, dosadašnji „klasični” proizvođači postaju multimedijalni predstavnici informacija koristeći se Internetom ili sopstvenom komercijalnom bazom podataka. Mora se imati u vidu da informacione tehnologije imaju niz prednosti koje se ogledaju u:

- modernizaciji poslovnih aktivnosti uz smanjenje broja zaposlenih,
- boljem finansijskom poslovanju preduzeća,
- racionalnom korištenju kapaciteta, resursa i energije,
- kvalitetnoj distribuciji materijala, roba i usluga.

Ovo sve utiče na poboljšanje položaja preduzeća u poslovanju. Informacione tehnologije bitno mjenjaju konkurentne izgledе svih poslovnih procesa tokom procesa proizvodnje, ali i u procesu pružanja usluga preduzeća.

## 2. TRENDOWI MOGUĆEG RAZVOJA U POSLOVNOM SISTEMU

Svi se slažemo da će novije mrežne tehnologije morati da budu različite od onih koje se sada koriste, dvje ili više odvojenih mrežnih tehnologija uslužuju obične kompjutere današnjice. Najčešće su to u pitanju telefonske mreže za glasovne komunikacije i LAN za komunikaciju sa podacima kompanija ili sa ostatkom svijeta. Spajanje ovih, sada odvojenih mreža, u jednu bi donijelo bezbroj koristi i priličnu uštedu. Koje bi karakteristike posjedovala takva mreža? Prije svega morala bi da bude univerzalna, fleksibilna i trebala bi da nudi poželjan kvalitet svojih servisa. Prva potreba implicira da mreža treba da bude pogodna za prenos svih tipova saobraćaja, druga treba da omogući korisnike da dinamički iskorištavaju kapacitete koji su potrebni i treća treba da omogućava korisnike da odaberu kvalitet servisa potrebnog za određeni prenos podataka i aplikacija. Ispod je lista kvalitetnih servisa potrebnih za određene tipove saobraćaja i aplikacija. Karakteristike novijih tehnologija:

- Pogodne za sve tipove saobraćaja
- Brze i pouzdane
- Lake za korištenje i upravljanje

- Razne usluge servisa.

U današnje vrijeme se najčešće poslovni podaci obrađuju na računaru, ali su se zadržali stari načini razmjene poslovnih informacija i dokumenata u papirnom formatu. Ako bi se mogućnosti postojećih računara i telekomunikacija iskoristile na pravi način mogle bi umnogome da unaprijede poslovanje istovremeno smanjujući troškove, pružajući bolje usluge i smanjile bi se greške do kojih dolazi u radu na klasičan način. Za naručivanje robe ili servisa tradicionalnim putem, narudžba se štampa i šalje poštom nabavljaču, račun se priprema, štampa, i šalje kupcu, i isplata se pravi preko čeka.

Preko 75% svih poslovnih dokumenata koje je štampala jedna organizacija se ručno prekucava u drugoj organizaciji! Sve veća upotreba Weba, Interneta, intraneta, ektraneta i elektronske trgovine mijenjaju način na koji se posluje u skoro svim organizacijama, stavljajući u prvi plan inovativne primjene informacione tehnologije. Internet, intranet i ektranet se mogu koristiti na više načina radi sticanja konkurentne prednosti u korporacijskom okruženju, ali najznačajnija poslovna inovacija se danas ogleda u doprinosu komunikaciji, saradnji i otkrivanju informacija.

Ova nova vrsta računarstva pomaže nekim inovativnim kompanijama da se istaknu, a drugima (koje su iz nekog razloga u krizi) jednostavno da opstanu. Intranet je neočekivani korak suprotan Internetu. U suštini to su mini-Internet-ovi koje su razvile pojedine organizacije ili grupe organizacija. Koristeći postojeća iskustva na Internetu započeta su istraživanja o tome šta se sve od Interneta može preuzeti, a šta dodatno napraviti da bi se na istom principu napravio softver, koji bi bio dovoljno pouzdan i zaštićen za poslovne primjene. Pošto se može predvidjeti da će svijet Intranet-a progresivno rasti u dužem vremenskom periodu, vjerovatno će i svakodnevna poslovna komunikacija između korisnika početi da dobija znatno drugačije i raznovrsnije oblike.

Kako se koncept intraneta širi, a hardver i softver podrške se standardizuju logično je pretpostaviti da će ga većina organizacija koristiti za internu komunikaciju. Infrastruktura intraneta je sputana granicama same firme, ali ne i geografskim; intranet se također može upotrijebiti za povezivanje kancelarija iste firme na različitim lokacijama

### 3. ELEKTRONSKO POSLOVANJE

Elektronsko poslovanje, poznatije kao e-Business, mora biti definisano kao određeni trgovinski proces, baziran na automatizovanom informacionom sistemu, što se danas najčešće realizuje uz pomoć naprednih Web tehnologija i sve većim brojem raspoloživih mrežnih servisa koji generalno olakšavaju sve procese koji posredno i neposredno opslužuju elektronsko poslovanje. Metode elektronskog poslovanja omogućavaju kompanijama povezivanje njihovih internih i eksternih sistema obrade podataka još efikasnije i fleksibilnije, u cilju veće zatvorenosti u odnosima sa dobavljačima i poslovnim partnerima i mnogo bolje zadovoljavanje potreba njihovih mušterija. U praksi, elektronsko poslovanje (e-Business) je mnogo više od elektronske trgovine (e-commerce). Elektronsko poslovanje stavlja akcenat na funkcijama koje se realizuju uz pomoć savremenih elektronskih dostignuća, dok je elektronska trgovina deo globalne strategije elektronskog poslovanja i teži da ostvari prihode putem World Wide Web-a, odnosno Interneta kako bi poboljšala veze sa klijentima i partnerima u cilju povećanja efikasnosti. Elektronsko poslovanje u širem smislu reči

predstavlja organizaciju poslovanja firme u mrežnom okruženju kao i organizovanje poslovne komunikacije i brigu o njima, dok se njegov uži smisao može odnositi na vođenje poslova na Internetu odnosno kupovinu i prodaju.

### 3.1. Perspektive razvoja elektronskog poslovanja

Razvoj Internet tehnologija imamo svuda u svijetu, pa je tako i našoj zemlji otvorena mogućnost da se integriše u već postojeće ili novostvorene sisteme elektronskog poslovanja. To je stvarno kompleksan proces koji zahtjeva angažovanje stručnjaka iz različitih oblasti i znatne novčane investicije. Da bi se elektronsko poslovanje moglo razvijati, potrebno je ispuniti neke tehnološke pretpostavke. Prije svega je potrebno raspolagati informatičkom magistralom tj. infrastrukturom zadovoljavajućeg kapaciteta.

Da bi se osigurala kompatibilnost uređaja i metoda koje se koriste u elektronskom poslovanju, potrebno je standardizovati sve aspekte rada mreže, od standarda video distribucije do protokola za rad u mreži i pružanja mrežnih usluga, kompresije različitih oblika multimedijalnih dokumenata i sl.

Osim tehnoloških preduslova potrebno je ostvariti i unaprijediti i zakonske pretpostavke koje će omogućiti nesmetan razvoj elektronskog poslovanja, zaštitu autorskih prava i privatnosti i osigurati univerzalni pristup mreži i adekvatnu politiku određivanja cena za pristup mreži i korišćenje informacija. „Zakon o elektronskom poslovanju i elektronskom potpisu“ koji je u fazi donošenja kod nas, je neophodan preduslov kako za pravnu zasnovanost elektronskog poslovanja tako i za uključenje u međunarodne organizacije i tokove. Među najvažnijim razlozima za optimistička predviđanja brzog razvoja elektronskog poslovanja su:

- izvanredno brz tehnološki razvoj,
- razvoj novih servisa i poslovnih modela,
- razvoj nacionalnih i međunarodnih standarda i vodiča za elektronsko poslovanje.

## 4. KRIPTOVALUTA

Bitcoin je prvi primjer kriptovalute. Kriptovaluta je digitalni ekvivalent novca koja funkcioniše na temelju kriptografskih algoritama. Jedinice valute zvane bitcoin koriste se za pohranu i prijenos vrijednosti među korisnicima u bitcoin mreži. Korisnici međusobno komuniciraju koristeći bitcoin protokol primarno putem Interneta, iako je moguć prijenos i drugim mrežama. Bitcoin algoritam je napisan kao open source program tako da svako može vidjeti kod. Bitcoin se može pokretati na raznim računarskim uređajima.

Za razliku od tradicionalnih valuta koje su imale pokriće u prirodnim dobrima, Bitcoin je u potpunosti virtualan. Ne postoji fizički niti digitalni novac kao takav. Novac je ut-kan u transakcije koje prebacuju vrijednost od pošiljalca do primatelja. Korisnici mogu prebaciti bitcoine putem mreže te sa njima obavljati gotovo sve što se može obavljati sa tradicionalnim valutama. To uključuje kupovinu i prodaju dobara, slanje novca ljudima ili organizacijama te ostvarivanje kreditne moći.

Bitcoin se mogu kupovati, prodavati i zamijeniti za ostale valute (u posebnim mjenjačnicama). U nekom smislu, bitcoin je savršen oblik novca na Internetu jer je brz, siguran i jednostavan za korištenje po cijelom svijetu. Korisnici bitcoina posjeduju ključeve

koji im omogućuju da dokažu vlasništvo transakcija u Bitcoin mreži, otključavajući vrijednost koju kasnije mogu potrošiti ili je proslijediti novom primatelju. Ti IDkjučevi su najčešće pohranjeni u digitalnim novčanicima na korisnikovom računaru. Posjedovanje ID kjuča koji otključava transakciju je jedini preduvjet za trošenje bitcoina čime se potpuna kontrola stavlja u ruke svakog korisnika.

Bitcoin se stvaraju kroz proces koji se naziva rudarenje (eng. mining). Rudarenje uključuje traženje rješenja matematičkog problema za vrijeme obrade bitcoin transakcije. Bilo koji sudionik bitcoin mreže može izvršavati funkciju rudara koristeći računarsku snagu svog računara. Ovi pojedinci ili tvrtke uljučuju se u aktivnosti održavanja Bitcoin mreže u zamjenu za transakcijske pristojbe i novonastale bitcoine.

Korisnici mogu slati i primati bitcoine elektroničkim putem bez naknade ili za neznatnu naknadu pomoću računarskih programa tzv. softverskih novčanika (eng. software wallet) koji se mogu nalaziti na osobnom računaru, mobilnom uređaju ili na internetu kao web aplikacija. Prosječno svakih deset minuta netko je u mogućnosti potvrditi transakcije u proteklih deset minuta i zbog toga je nagrađen novim bitcoinima. Upravo zbog rudarenja bitcoin je decentralizirana valuta te kao takva nije pod kontrolom niti jedne središnje banke.

Bitcoin protokol uključuje ugrađene algoritme koji reguliraju funkciju rudarenja. Složenost problema kojeg rudari moraju riješiti da bi uspješno potvrdili blok transakcija je dinamički prilagođena tako da netko uspije svakih deset minuta neovisno o tome koliko je rudara uključeno u proces. Protokol usporava brzinu stvaranja novih bitcoina za pola svake četiri godine i ograničava ukupan broj bitcoina koji će biti stvoreni na dvadeset jedan milijun. Taj broj biti će dostignut otprilike 2140. godine.

Zbog ove ograničene rate izdavanja novih bitcoina, bitcoin ne može doživjeti inflaciju. S obzirom na to da bitcoin ne može pobjeći iz bitcoin mreže, i kako su sve transakcije transparentne, puno je veća vjerojatnost da će bitcoin biti podložan deflaciji. Trenutna vrijednost bitcoina iznosi oko 300\$ i podložna je promjenama vrijednosti na dnevnoj bazi, a kroz vrijeme vrijednost bi mu trebala biti stabilnija.

## 5. DIGITALNI POTPIS

Digitalni potpisi (eng. digital signature - DS) omogućuju utvrđivanje autentičnosti elektroničkog dokumenta, npr. elektroničkog pisma, web stranice ili slikovne datoteke. Dokument je autentičan ako je poznat njegov autor i ako je moguće dokazati da nije neovlašteno izmijenjen.

Provjera vjerodostojnosti (eng. authentication) potpisanih dokumenata omogućena je korištenjem enkripcije, pri čemu enkripcija predstavlja postupak kodiranja podataka prije slanja kako bi ih samo ovlašteni primatelj mogao dekodirati i razumjeti. Uz to što osigurava autentičnost (identitet pošiljatelja utvrđuje se dešifriranjem sažetka poruke), digitalni potpis osigurava i integritet (provjerom sažetka poruke utvrđuje se je li se poruka mijenjala na putu do primatelja) te neporecivost (pošiljatelj ne može poreći sudjelovanje u transakciji jer jedino on ima pristup do svog privatnog ključa kojim je potpisao poruku).

Korištenjem algoritma digitalnog potpisa potpisnik stvara par ključeva, privatni i javni, ali moguće je i da se za potpisivanje svih poruka koristi isti par. Poruka koju se potpisuje sažima se nekim hash algoritmom – stvara se njezin otisak. DS algoritam iz tako dobivenog sažetka poruke i korisnikova privatnog ključa stvara digitalni potpis koji se šalje ili objavljuje zajedno s potpisanom porukom.

Osnova sigurnosti digitalnog potpisa je u tajnosti privatnog ključa dok je javni ključ svima dostupan, a omogućuje provjeru autentičnosti poruke. U nastavku dokumenta opisan je povijesni razvoj digitalnog potpisa, dan je općeniti prikaz načina rada te detaljniji opis triju popularnih DS algoritama. Osim toga, navedene su primjene digitalnih potpisa te je dan pregled mogućih napada s dva primjera. Dokument je zaključen objašnjenjem politike upravljanja digitalnim potpisima i prognozom njihova budućeg razvoja.

### 5.1. Primjena digitalnog potpisa

U nekoliko zemalja digitalni potpis ima status sličan onomu tradicionalnog pisanog potpisa. To znači da digitalno potpisani dokument potpisnika pravno obvezuje, u skladu s uvjetima navedenim u spomenutom dokumentu. Zbog toga se preporučuje korištenje različitih parova ključeva za enkripciju i za potpisivanje. Korištenjem para ključeva namijenjenih enkripciji, korisnik može sudjelovati u kriptiranoj komunikaciji (npr. pregovorima o kupnji nekretnine), ali ne potpisuje svaku poruku pravno važećim potpisom. Jednom kada zainteresovane strane postignu dogovor, ugovor se digitalno potpisuje i tek tada su potpisnici pravno vezani potpisanim dokumentom. Tako potpisani ugovor moguće je zatim, zbog dodatne zaštite, slati kriptiranog.

DS algoritmi i protokoli ne pružaju, sami po sebi, informaciju o tome kada je dokument potpisan. Potpisnik može, ali i ne mora, uključiti vremensku oznaku (eng. time stamp) unutar digitalnog potpisa ili se u samom dokumentu može spominjati datum i vrijeme potpisivanja. Ovakvo označavanje vremena omogućuje navođenje netačnog, npr. ranijeg datuma ili vremena potpisivanja. Korištenje sigurnih vremenskih oznaka (eng. trusted time stamp) sprečava se ovakva zloupotreba digitalnog potpisa. Sigurne vremenske oznake osigurava pouzdana treća strana, tzv. TSA (eng. TimeStamping Authority), koja time potvrđuje postojanje određenih podataka prije nekog vremena. Ranjivosti takvog korištenja vremenskih oznaka moguće je umanjiti umetanjem više oznaka različitih TSA organizacija u potpis. Jedna od osnovnih prednosti korištenja digitalnih potpisa, uz osiguravanje autentičnosti i integriteta dokumenta, je onemogućavanje nepriznavanja dokumenta od strane potpisnika (eng. nonrepudiation).

Ako sporna poruka nije potpisana, njezin ju navodni pošiljatelj uvijek može zaniijekati tvrdnjama kako ju je netko drugi napisao i poslao. Takvo što se ne može dogoditi s potpisanim porukama osim u slučaju otkrivanja korisnikovog privatnog ključa, kojeg zbog toga treba čuvati u strogoj tajnosti. Spremanje privatnog ključa na tzv. pametnoj kartici (eng. smart card) jedan je od načina osiguravanja njegove tajnosti. Alternativa je čuvanje privatnog ključa na osobnom računar u korisnika, ali takav pristup ima dva ozbiljna nedostatka:

- korisnik može potpisivati dokumente samo na spomenutom računar u
- tajnost privatnog ključa ovisi o sigurnosti računara na kojemu je pohranjen.

Karticu je potrebno povezati na računar i proslijediti joj hash vrijednost poruke, ugrađeni procesor zatim iz pohranjenog privatnog ključa i primljenog otiska poruke proračunava potpis koji se potom šalje računaru. Na taj način privatni ključ nikada ne napušta karticu. Većinu kartica potrebno je prije upotrebe aktivirati osobnim identifikacijskim brojem (eng. Personal Identification Number – PIN), a građane su tako da onemogućavaju, ili barem otežavaju, neovlašten pristup pohranjenim podacima.

## 5.2. Budućnost digitalnog potpisa

Ako se nastave današnji trendovi u korištenju digitalnog potpisa oni će s vremenom potpuno zamijeniti pisane potpise u primjenama od dugoročnih korporativnih ugovora do osobnih pisama i dnevnika. Mnogi računarski stručnjaci slažu se kako će, kroz određeno vrijeme, za pokretanje svih programskih paketa i pristup svim datotekama biti potreban odgovarajući digitalni potpis.

Povećanje učestalosti primjene i važnosti digitalnog potpisa iziskuje standardizaciju algoritama koji ih implementiraju i to na razini država, na razini Interneta te od strane organizacija kao što su IEEE (eng. Institute of Electrical & Electronics Engineers) i ANSI (eng. American National Standards Institute).

Prednosti DS algoritama koji koriste eliptičke krivulje vjerojatno će rezultirati porastom njihove popularnosti i postupnim istiskivanjem drugih algoritama iz uporabe. Sve veće prihvaćanje digitalnog potpisa kao ravnopravne zamjene pisanog potpisa porasti će i učestalost pokušaja zlouporabe, pa je zbog toga potrebno razvijati sigurnosne mehanizme kojima bi se to spriječilo. Prije svega se to odnosi na korištenje sklopovskih rješenja za čuvanje privatnog ključa.

## ZAKLJUČAK

Analizirajući savremeno poslovanje i nove ekonomske trendove može se reći da su informacione tehnologije u svakom smislu sastavni element svakog biznisa i svake ozbiljne kompanije. Njihov uticaj se vidi u proizvodnji, marketingu, računovodstvu, istraživanju, razvoju i gotovo svim poslovnim funkcijama. Od prostih softverskih rješenja, pa do onih koji su u mogućnosti da integrišu čitav poslovni sistem, pa čak i onih za koje se iz ove perspektive može reći da pariraju menadžerovom odlučivanju informacione tehnologije su zaista revolucionarna pojava cjelokupnog našeg društva. Pored toga što su utjecale na promjenu poslovnog okruženja i poslovnih procesa, nove tehnologije utiču i na kreiranje potpuno novih vrijednosti u našem društvu. Uzimajući u obzir da se većina poslovnih inovacija odnosi baš na informacione tehnologije, možemo reći da su baš one zaslužne i nositelji su stvaranja nove vrijednosti u ekonomiji.

Pred nama je vrijeme potpune digitalizacije i uplitanja informacionih tehnologija u svaki segment našeg života. Uz pomoć informacione tehnologije u proteklih tridesetak godina razvijena su nova, naprednija, sistematičnija menadžerska znanja. Uvođenjem novih sistema u poslovanje, poslovno odlučivanje dobija jednu novu dimenziju. Svakom problemu se pristupa na detaljniji i analitičniji način te se uz pomoć računarske tehnologije odluke donose na lakši način. Zasigurno je da poznavanje i korištenje naprednijih informacionih tehnologija znači i obavljanje biznisa na efektivniji, produktivniji i konkurentniji način.

## LITERATURA

- [1] Informacione tehnologije - Poslovne komunikacije, Milan Kukrika – eMagazin
- [2] Reinženjering poslovnih procesa i informatičke tehnologije, Doc.dr Zvonko Sajfert,dipl.ing.org. , Mr Milan Nikolić, dipl. ing. za raz. , zbornik radova na stručnom skupu
- [3] Analiza i poboljšanje poslovnih aktivnosti upotrebom informacionih tehnologija, Siniša MinićMiloš Vorkapić , Dragan Kreculj
- [4] Internacionalna Konferencija, Teh. fakultet Čačak, 7–9. maj 2010.
- [5] Istorijat razvoja računarskih sistema
- [6] William Stallings: Cryptography and Network Security Principles and Practices, 4 izdanje, 2005.
- [7] Don Johnson, Alfred Menezes, Scott Vanstone: The Elliptic Curve Digital Signature Algorithm (ECDSA), Certicom Research, 2001
- [8] RSA Laboratories: RSA Cryptography Standard, 2002.
- [9] Infomosaic Corporation: Digital Signature in a Web Application, DoD PKE Forum Fall 2005, Atlanta

