# Sadržaj

[Sadržaj 1](#_Toc441336147)

[INFORMACIJA I INFORMACIJSKA KRIZA 4](#_Toc441336148)

[INFORMACIJA 4](#_Toc441336149)

[INFORMACIJSKA KRIZA 4](#_Toc441336150)

[UZROCI informacijske krize: 4](#_Toc441336151)

[Informacijska i informatička pismenost 5](#_Toc441336152)

[Utjecaji informacijske tehnologije na poslovnu politiku poduzeća: 5](#_Toc441336153)

[Sustavni pristup 6](#_Toc441336154)

[Vrste sustava 7](#_Toc441336155)

[Informacijski sustav 7](#_Toc441336156)

[Funkcije IS: 8](#_Toc441336157)

[Strukturu IS čini: 8](#_Toc441336158)

[Izgradnja IS poduzeća 10](#_Toc441336159)

[Elektronička razmjena podataka (EDI) 12](#_Toc441336161)

[EKSPERTNI SUSTAVI 14](#_Toc441336162)

[Baza znanja 15](#_Toc441336163)

[Glavne karakteristike ekspertnog sustava: 15](#_Toc441336164)

[OSIGURANJE I ZAŠTITA PODATAKA 16](#_Toc441336168)

[Metode osiguranja i zaštite podataka u IS 17](#_Toc441336169)

[Svojstva biometrijskih metoda 17](#_Toc441336170)

[KAKO ZAŠTITITI SVOJE RAČUNALO 19](#_Toc441336171)

# INFORMACIJA I INFORMACIJSKA KRIZA

* živimo u svijetu u kojem dominiraju tehnologija, informacije i znanje

## INFORMACIJA

* + podatak kojem čovjek pripisuje značenje
	+ podatak koji služi za donošenje odluka
	+ podatak koji povećava znanje primatelja

Informacije za razliku od materije i energije imaju specifična obilježja:

* + Ne troše se uporabom
	+ Ne smanjuju se raspodjelom.

Cjelokupno ljudsko znanje:

* nastalo do 1900.g. udvostručuje se već 1950.g.
* a nakon toga količina znanja udvostručuje se svakih par godina.

Eksplozija znanja stvara informacijsku krizu.

## INFORMACIJSKA KRIZA

* Nemogućnost sustava da na zadovolji svoje potrebe za informacijama
* Da upravlja informacijama
* Da održi i automatizira prikupljanje, pohranjivanje, obradu, pretraživanje i uporabu informacija

Knjige i pisani materijali nisu dobri oblici za spremanje velike količine podataka i informacija. Dio cjelokupnog znanja pretvara se u:

* Softver (program za knjiženje, obračun plaća, ispis svjedodžbi, vođenje skladišnje evidencije, itd.)
* Hardver (inteligentni strojevi koji u potpunosti zamjenjuju rad čovjeka- bankomati, roboti, aut. telefonske centrale, proizvodni pogoni)

## UZROCI informacijske krize:

* Velika količina informacija
* Porast složenosti i raznolikosti problema – nastoji se riješiti informatizacijom.
* Razvoj programskih proizvoda (visoka cijena)
* Problem upravljanja u organizacijskim sustavima

# Informacijska i informatička pismenost

Informacijska pismenost – uviđanje potrebe za informacijom te posjedovanje znanja o tome kako pronaći, procijeniti i iskoristiti najbolje i najnovije informacije.

Izvori informacija mogu biti različiti:

* knjige
* časopisi
* računala
* TV
* Internet
* informacijski pismena osoba je ona koja zna kako učiti, zna kako pronaći informacije i kako se njima koristiti
* osoba pripremljen za cjeloživotno učenje

Informatički pismena osoba je osoba koja razumije ulogu računala u procesu traženja informacija

* uspješno traženje informacije ovisi o osobi, a ne o tehnologiji kojom se koristi

Znanja koja treba posjedovati informatički pismena osoba – stalno se dopunjuju jer moraju pratiti brz razvoj informacijske i komunikacijske tehnologije.

* prije nekoliko godina (poznavanje konfiguracije računala, osnove korištenja OS i programa za obradu teksta)
* danas ( korištenje Interneta, rad s elektroničkom poštom, pretraživanje web-a, stavljanje vlastitih sadržaja na web, poznavanje programa za izradu multimedijskih prezentacija, itd)

Veliki broj zaposlenih neovisno o poslovima koje obavljaju, u svom radu koriste suvremenu informacijsku tehnologiju.

## Utjecaji informacijske tehnologije na poslovnu politiku poduzeća:

1. informacijska se tehnologija ugrađuje u sve veći broj proizvoda i usluga
2. kreiranje novih proizvoda i usluga
3. mijenjaju se poslovni odnosi
4. u definiranju poslovne strategije važno je dalekovidno sagledati trendove (nastaju promjene koje zahtijevaju redefiniranje proizvoda, usluga, djelatnosti i cijelih grana privređivanja)
5. smanjuje troškove poslovanja
6. upravljanje na temelju kvalitetnih usluga

Nove tehnologije rezultirale su pojavom novih poslova, novih zanimanja kao i novih načina njihova obavljanja.

# Informacijska zanimanja

Ljudi

1. korisnici

 menadžer – za donošenje odluka

službenici (izvršitelji) – za obavljanje svakodnevnog posla

 2. profesionalni informatičari:

 a) programeri – pišu i održavaju korisničke programe

 b) projektanti IS – istražuju potrebe korisnika

 c) administratori baze podataka – razvijaju i održavaju baze podataka

 d) administratori mreža – brinu se o ispravnosti mreže

 e) web page administratori – kreiraju i razvijaju informacijske usluge preko

 interneta

 f) operateri – upravljaju sklopovljem, provode standardne procedure, izvode

 programe koji su programeri napravili

Informatičari sudjeluju na izobrazbi ostalih kadrova, održavaju informatičke mreže, itd.

# Sustavni pristup

Postoje tri pristupa u izučavanju predmeta i pojava:

1. opservacijski ili opažajni pristup – sastoji se od opažanja i zatim detaljnog opisivanja uočenog.
2. analitički pristup – svaki problem promatra se kao skup neovisnih elemenata, koji treba rastaviti na dijelove da bi pojava u cijelosti mogla biti shvaćena
3. sustavni pristup – primjenjuje se na vrlo složene sustave, taj pristup naglašava analizu procesa, a ne komponente tog sustava, te u središte istraživanja postavlja proces. Svi predmeti i pojave promatraju se kao sustavi.

Svuda oko nas nalaze se sustavi. Sustav je cjelina koja se ne može rastaviti na svoje elemente, a da se pritom ne izgube njezine osnovne karakteristike.

Sustav je skup međusobno povezanih elemenata koji čine jednu cjelinu i koji svojim funkcioniranjem ostvaruju zajednički cilj ili ciljeve.

Sustav koji je povezan sa svojom okolinom crpi iz nje materiju, energiju i informacije potrebne za svoj opstanak i razvoj.

Svaki sustav ima 4 komponente (osnovni model sustava): ulaz, proces, izlaz i povratna veza.

proces

ulaz

izlaz

povratna veza

Funkcioniranje sustava izražava se kao pretvaranje ulaznih veličina u izlazne. Zadatak je povratne veze kontrola izvršenja planiranih aktivnosti . Usporedbom planiranog i ostvarenog uočavaju se odstupanja pa se u slijedećem ciklusu vrši ispravak djelovanja sustava kako bi se ostvario planirani cilj.

# Vrste sustava

1. Prema vrsti elemenata od kojih su građeni:
	1. Apstraktni sustavi – čiji su elementi povezani pravilima i definicijama (brojevni sustavi, komp. Programi, ljudski govor, periodni sustav elemenata…)
	2. konkretni sustavi – imaju svoju fizičku pojavnost (računalo, stroj, automobil…)
2. prema složenosti sustava
	1. jednostavni – imaju konačan broj elemenata koji su povezani jednostavnim vezama
	2. složeni – sustav gospodarstva RH, mirovinski sustav, nacionalno tržište dionica
3. prema odnosu s okolinom
	1. otvoreni – primaju materiju, energiju i informacije iz okoline i šalju ih u nju
	2. zatvoreni – nemaju ni ulaza ni izlaza
4. prema načinu ponašanja
	1. statički – ne mijenjaju strukturu ni funkcioniranje u vremenu
	2. dinamički mijenjaju se u vremenu
5. prema mogućnosti predviđanja budućeg ponašanja
	1. deterministički – u potpunosti se može predvidjeti buduće ponašanje jer djeluju u skladu s unaprijed poznatim pravilima (računalni programi, sustav dvije jednadžbe itd.)
	2. stohastički sustavi - čije ponašanje nije predvidivo već ga možemo samo prognozirati(poslovanje poduzeća, gospodarski i društveni sustav).
6. prema naravi sustava
	1. prirodni – sustav rijeka, sunčev sustav
	2. umjetni – obrazovni sustav, sustav prometnica, mreža računala
	3. kombinirani – sustav navodnjavanja

Svojstva mnogih sustava nisu jednoznačna.

# Informacijski sustav

- poduzeće razmjenjuje velike količine podataka s okolinom

IS je onaj sustav koji:

- osigurava informacije za potrebe poslovanja,

- nedjeljiv dio svakog upravljanog sustava ,

- omogućuje sve poslovne procese u poduzeću

IS možemo opisati odgovorima na tri pitanja:

1. Što mu je cilj ili svrha?
2. Koje su mu funkcije?
3. Od čega se sastoji ?

Cilj ili svrha IS je dostaviti pravu informaciju u pravo vrijeme na pravo mjesto uz što niže troškove.

## Funkcije IS:

1. prikupljanje podataka – iz samog poslovnog sustava i okoline
2. obrada podataka – podaci se obrađuju prema potrebama korisnika (preoblikuju, sažimaju ili rasčlanjuju)
3. pohranjivanje podataka – podaci se pohranjuju radi kasnije uporabe ili se dostavljaju korisnicima za potrebe upravljanja, odlučivanja i kontrole.
4. dostava podataka i informacija korisnicima ( u različitim oblicima)

## Strukturu IS čini:

* hardver – računala i sve periferne jedinice kojima se obavlja prikupljanje, obrada, memoriranje i distribucija podataka korisnicima
	+ računala se dijele na:
		- superračunala
		- mainframe
		- srednja računala
		- mikroračunala (stolna, prijenosna, dlanovnici;PDA)
* softver -skup svih programa koji se koriste u IS
* sustavski – skupina programa koja je:
 - neposredno povezana sa pokretanjem računala
 - i osnovnim funkcijama računala
	+ - * operativni sustavi
			* upravlja cjelokupnim radom računala,
			* svim strojnim komponentama
			* i omogućava izvršavanje korisničkih programa
			* pogonski programi (driver) – programi koji upravljaju jedinicama računala koje su:
				+ ugrađene ili priključene na računalo
			* pomoćni programi ili uslužni programi – pomažu operacijskom sustavu u izvršavanju dodatnih poslova (provjera ispravnosti diska, defragmentacija, stvaranje sigurnosne kopije, itd.).
	+ aplikacijski
		- * vlastiti
			* kupljeni
* Lifeware (ljudi)
	+ korisnici IS rade s informacijama i rezultate obrade koriste za rad ili unaprjeđenje svog posla
		- menadžeri
		- izvršitelji
	+ profesionalni informatičari – osmišljavaju, razvijaju i održavaju IS
* Mreže

Računalna mreža ima nekoliko temeljnih funkcija:

o Funkcija suradnje – povezivanje računalnih procesa u cjelinu prilikom izvršavanja raspodijeljenih zadaća

o Funkcija povezivanja – komunikacijsko povezivanje udaljenih partnera

o Funkcija prijenosa podataka – pouzdan prijenos podataka između udaljenih sustava.

Podjela mreža prema udaljenosti

o **Lokalne mreže** (LAN – Local Area Network) – mreže kratkog dosega koje tipičnopovezuju računala unutar jedne zgrade ili kompleksa zgrada

o **Gradske mreže** (MAN – Metropolitan Area Network) – lokalne mreže srednjegdosega koje se koriste za povezivanje pojedinačnih lokalnih mreža u veće cjeline naširim gradskim područjima

o **Globalne mreže** (WAN – Wide Area Network) – mreže koje povezuju lokacije na velikim udaljenostima, a tipično su izgrađene nad već postojećom globalnom telekomunikacijskom infrastrukturom (telefonske parice, optička vlakna...).

Prema ulozi računala u mreži razlikujemo :

* **Klijentsko – serverske mreže**
* **Čvor – čvor (Peer-To-Peer)**
	+ Priključena računala su međusobno ravnopravna
	+ svako računalo može biti i poslužitelj i klijent
	+ Pogodno za manja poduzeća ili kućnu upotrebu

Poslužitelj – korisnik (Server/Client)

* + Jedno glavno i više manjih računala
	+ računalo na koje se smještaju zajednički podaci i resursi
	+ Pogodno za veće organizacije i sustave
	+ poslužitelj ima zadaću primati zahtjeve i podatke, obraditi podatke sukladno zahtjevu korisnika i poslati obrađene podatke natrag korisniku
	+ poslužitelj je udaljeno računalo koje korisnik fizički ne vidi

Internet je najpoznatiji primjer client-server mreže



Podjela mreža prema topologiji:

- podrazumijevamo fizički raspored računala

* Star mrežna topologija se sastoji od središnjeg čvora na kojega su kablovima direktno spojeni ostali čvorovi na mreži



* Bus (sabirnica, crta) topologija se sastoji od centralnog vodiča na koji su spojeni čvorovi koji komuniciraju



* Ring topologija se sastoji od čvorova koji su povezani samo sa dva susjedna čvora, a prvi i posljednji su međusobno povezani tvoreći fizički krug



* Tree topologija se sastoji od centralnog čvora koji je najviši u hijerarhijskom rasporedu čvorova i na njega spojenih čvorova koji se nalaze na sloju niže od njega.



* Mesh topologija se sastoji od čvorova koji mogu imati direktne veze sa više ili sa svim čvorovima u mreži.



* Dataware IS-a sadržan je u podacima, informacijama i znanju.
* Organizacija- se podrazumijeva organizacija tehničke opreme, programske opreme IS-a (software) i ljudi

Razlikujemo više oblika organizacije IS:

o Odjel za informacijski sustav

o Korisničko računalstvo

o Informacijski centar

o Unajmljivanje informacijskih usluga (Outsourcing)

**Izgradnja IS poduzeća**

IS poduzeća ima dvije funkcije

1. **funkcija dokumentiranja** -daje dokumentaciju na temelju koje radnici i vanjske organizacije imaju uvid u poslovanje poslovnog sustava

2.**funkcija informiranja** – služi za potrebe upravljanja i odlučivanja

**ZADATAK IS** poduzeća je osigurati informacije za potrebe upravljanja, odlučivanja i kontrole radi donošenja ispravnih poslovnih odluka.

***Izgradnja IS provodi se metodom:***

1. improvizacije
- polazi se od rješavanja problema i pisanja aplikacija onako kako ih nameće potreba, slučaj ili odluka voditelja
- kreće se od dijelova prema cjelini
- svaka aplikacija funkcionira uspješno za sebe
- razvijanjem sustava javlja se potreba za povezivanjem pojedinih dijelova, i tada nastaju problemi (aplikacije nastale za sebe i na različitoj opremi teško je ako ne i nemoguće povezati u jednu cjelinu
2. sustavskom metodom – najprije se definiraju obilježja cjeline , a tek zatim se prelazi na realizaciju pojedinih dijelova.
Sastoji se od 7 faza projektiranja i izgradnje IS (koje se još nazivaju i faze životnog ciklusa IS):
1. Strategija informatizacije i dugoročno planiranje
2. Analiza postojećeg sustava
3. Definiranje zahtjeva postavljenih pred novi sustav
4. Oblikovanje novog sustava
5. Razvoj novog sustava
6. Implementacija (uvođenje u rad) novog sustava
7. Ocjena uspješnosti i održavanje novog sustava

1. Strategija informatizacije i dugoročno planiranje
utvrđuju se :

1. Nedostaci i problemi postojećeg sustava
2. Strateški utjecaj informatizacije na temeljnu djelatnost
3. Cilj novog sustava
4. Kadrovski, organizacijski i financijski aspekti novog sustava
5. Plan razvoja novog sustava

2. Analiza postojećeg sustava: - analiziraju se:
ulazni podaci

* + izlazni podaci
	+ datoteke
	+ postupci i metode rada
	+ način pohranjivanja podataka
	+ postupci kontrole
	+ te postojeći hardver i softver

3. Definiranje zahtjeva postavljenih pred novi sustav

* što će novi sustav raditi i kako

4. Oblikovanje novog sustava

* Ima tri cilja:
	+ Izraditi detaljan opis novog sustav i način njegova funkcioniranja
	+ Stvoriti okvir kontrole u kojem će novi sustav djelovati
	+ Napraviti dokumentaciju za razvoj novog softvera

5. Razvoj novog sustava

* u toj fazi izrađuje se aplikacijski softver (dio se može izraditi dok se dio može i kupiti)

6. Implementacija (uvođenje u rad) novog sustava

* glavni zadatak je naučiti korisnika kako se svakodnevno koristiti novom tehnologijom i novim metodama
* kreiranje dokumentacije
* konvertiranje postojećih datoteka u novi sustav
* testiranje cijelog sustava – sa stvarnim podacima

Načini prelaska starog u novi sustav

1. istovremeno funkcioniraju stari i novi sustav
2. fazno uvođenje novog sustava
3. prestaje s radom i počinje korištenje novog sustava
4. dok funkcionira stari napravi se model novog sustava i provjerava sposobnost novog na modelu

7. Ocjena uspješnosti i održavanje novog sustava

1. provjeriti ispunjava li novi sustav zahtjeve ( preporuke za poboljšanja)
2. održavanje novog sustava- novi sustav treba prilagođavati promjenama koje mogu biti:
	1. normativne (promjena zakona)
	2. tržišne (novi proizvodi ili usluge)
	3. tehnološke (novi hardver ili softver)

# Elektronička razmjena podataka (EDI)

* electronic dana interchange
* bitna komponenta modernog IS
* u današnje vrijeme poslovni podaci se obrađuju na računalu ( ponegdje se zadržao stari način razmjene posl. informacija i dokumentacije u papirnatom obliku)

EDI je sustav:

* razmjene poslovne dokumentacije
* u dogovorenom, standardiziranom obliku
* putem računala
* između različitih organizacija

Prvi oblici edi pojavljuju se početkom 70-tih godina kada banke uspostavljaju sustav elektroničkog prijenosa gotovine, a u gospodarstvu i državnoj upravi nekoliko godina poslije

Edi utemeljena je na EDI normama (EDIFACT)

* EDIFACT standard – dogovor o tome kako podaci moraju biti pripremljeni za elektroničku komunikaciju
* Koristi ga mali broj poduzeća zbog visokih troškova uvođenja
	+ nabava opreme,
	+ prihvaćanje tehničkih normi,
	+ povezivanje računala između organizacija,
	+ obrazovanja korisnika, itd.

Primjena elektroničke razmjene podataka:

* + - Kupnja i prodaja proizvoda i usluga
		- Narudžbe, porezni obrasci, dozvole
		- Širenje javnih informacija

Prednosti EDI-ja

* Smanje troškova obrade papirnate dokumentacije
* Skraćenje vremena za naručivanje
* Dostava dokumenata u roku od nekoliko sekundi
* Mogućnost elektroničkog slanja računa i elektroničkog plaćanja
* Smanjenje ljudskih grešaka u OP

Dolaskom Interneta Edi postaje dostupna i najmanjim poduzećima, poduzeća mogu komunicirati putem javne mreže (Interneta), Intraneta i Extraneta.

Najvažnija su područja elektroničkog poslovanja:

* B2B – business to business – poslovanje između tvrtki
* B2C – business to consumer – između tvrtki i krajnjih kupaca

Elektroničko je poslovanje na Internetu prošlo nekoliko faza:

* Predstavljanje poduzeća na mreži
* Prikaz kataloga robe i usluga
* Prikupljanje zahtjeva kupaca
* preuzimanje narudžbi
* prodaja robe pojedincima (B2C)
* poslovanje između tvrtki (B2B)

# EKSPERTNI SUSTAVI

* su programi temeljni na znanju iz nekog specijalističkog područja
* u tom području postižu kvalitetu i efikasnost rasuđivanja eksperata te pomažu u rješavanju problema
* pripadaju području umjetne inteligencije.

Inteligentni sustav svaki sustav koji pokazuje sljedeća svojstva:

1. **Pokazuje prilagodljivo ciljno usmjereno ponašanje**
2. **Uči na temelju iskustva**
3. **Koristi velike količine znanja,**
4. **Pokazuje svojstava svjesnosti,** objašnjavanja svojeg ponašanja,
5. **Komunicira sa čovjekom prirodnim jezikom i govorom**
6. **Tolerira pogreške i nejasnoće u komunikaciji**
7. **Odgovara u stvarnom vremenu**

Ekspertni sustavi rade na sličan način kao eksperti te koriste činjenice, znanje i rasuđivanje kod rješavanja problema.

Slika 1: Struktura ekspertnog sustava

## Baza znanja

- Sadrži sva znanja iz sustava za koji je namijenjen

- znanje je informacija o svijetu koja ekspertu omogućuje donošenje odluke

- znanje se najčešće prikazuje u obliku pravila.

(npr.: “AKO poduzeće ima narudžbi I ne uspijeva ih zadovoljiti, TADA treba zaposliti još radnika )

Baza činjenica

* sadrži činjenice o stanju specifičnog problema koji se upravo rješava te o toku rješavanja tog problema (npr. rezultate dosadašnjih pokušaja prevladavanja nelikvidnosti).
* mijenja sadržaj tijekom vremena kako se mijenja stanje problema.
* Činjenice mogu prikazivati privremeno ili trajno znanje.

Prim. dviju činjenica koje prikazuju privremeno i trajno znanje:

 Stopa inflacije je 7.6%. (privremeno znanje)
 Mjed je legura koja sadrži bakar i cink (trajno znanje)

**baza činjenica**

**baza znanja**

**mehanizam zaključivanja**

**korisničko sučelje**

**Mehanizam zaključivanja predstavlja mehanizam za traženje rješenja problema.**

# Glavne karakteristike ekspertnog sustava:

## jednostavno dodavanje novih znanja;

## visoki stupanj rješavanja problema:

## mogućnost objašnjenja što je napravljeno i zašto je napravljeno.

Prednosti koje pružaju ekspertni sustavi:

* sinteza znanja većeg broja ljudskih eksperata
* nema utjecaja umora i emocija
* neograničen vijek trajanja.

Značajna područja primjene su:

* medicinska, elektronička i elektromehanička dijagnostika
* planiranje prihoda, financije, bankarstvo (odobravanje kredita)
* procjena rizika u osiguranju
* planiranje eksperimenata u biologiji, kemiji, genetici
* oblikovanje računalnih sustava
* edukacijski sustavi
* Inteligentni roboti koji imaju sposobnost učenja

# OSIGURANJE I ZAŠTITA PODATAKA

* među najvažnijim pitanjima izgradnje IS
* velike računalne mreže i baze podataka nije lako zaštititi od krađe i zlouporabe podataka

Izvori opasnosti u IS

|  |  |
| --- | --- |
| Prirodni | Ljudski |
| namjerni | Nenamjerni (pogreška) |
| Požar | teroristi | Uništenje medija |
| poplava | Nezadovoljni djelatnici | Brisanje podatka |
| Sunčeva svjetlost, prašina … | hakeri | Nestručno rukovanje, nemar, nepažnja, neznanje,… |

Pred IS se postavljaju 3 zahtjeva kojima treba udovoljiti:

1. sigurnost – u IS trebaju postojati uvjeti u kojima neće biti ometana ni jedna njegova funkcija. Sigurnost može biti ugrožena na različite načine.
2. zahtjev raspoloživosti – pristup podacima i informacijama mora biti omogućen prema ovlaštenjima. Treba precizno odrediti koje su osobe ovlaštene za obavljanje transakcija, tko smije imati uvid u određene podatke, tko obavlja brisanje, mijenjanje i kopiranje podataka,…
3. zahtjev tajnosti – ima dva aspekta:
1. informacije koje se smatraju povjerljivima – valja podvrgnuti posebnom režimu zaštite i staviti na raspolaganje uskom krugu korisnika (poslovna tajna)
2. privatni podaci i informacije o osobama – treba zaštititi od bilo čijeg neovlaštenog uvida

## Metode osiguranja i zaštite podataka u IS

1. metoda identifikacije – zaštita od neovlaštenog pristupa nekom dijelu IS. Svaki korisnik mora se fizički ili logički identificirati prije nego što obavi bilo kakvu transakciju.
fizička identifikacija – uz pomoć nekog predmeta ( ključa ili kartice) ili biometrijske metode (boja glasa, potpisa, DNK, šarenica oka, otisak prsta, uha itd…)
logička - (temelji se na lozinci ). Biometrija se u počecima razvijala uz slogan: “The body as password”.

Korisničko ime i šifre najčešće se rabe za pristup operativnim sustavima. Šifre su u pravilu jednostavne i sastoje se od imena, prezimena ili datuma rođenja, što svaki bolji haker može 'provaliti'. Program studenata iz Varaždina, međutim, detektira brzinu tipkanja, tako da, čak i ako netko zna korisničko ime i šifru, neće moći ući u računalo jer ne tipka posve isto kao njegov korisnik

2. metoda provjere ovlasti – korisnik može obavljati samo one poslove za koje je ovlašten (pristup bazi, prijenos podataka, uporaba određenih programa,…)

1. metoda zaštite u prijenosu – temelji se na fizičkoj izolaciji kanala komuniciranja ili na primjeni standardnih protokola koji imaju ugrađene mehanizme zaštite.
2. kriptografske metode – koristi se za podatke koje treba posebno zaštititi (vojne tajne, recepti itd.
temelji se na dvije faze:
- kriptiranje – pretvaranje izvorne riječi u tajnu
- dekriptiranje – šifrirane se poruka primjenom algoritma pretvara u izvorni oblik

## Svojstva biometrijskih metoda

1. Univerzalnost je kriterij koji se odnosi na udio osoba koje posjeduju karakteristiku potrebnu za autentifikaciju.
2. Jedinstvenost: Bilo koje dvije osobe ne bi smjele imati jednake biometrijske karakteristike.
3. Trajnost karakteristike znači da se ne bi smjela mijenjati s vremenom. Karakteristike kao šarenica oka ili termogram lica tokom vremena ostaju nepromijenjene. Lice osobe, glas ili karakteristike ponašanja mijenjaju se starenjem osobe.
4. Prikupljivost znači da se karakteristika može lako izmjeriti i kvantitativno izraziti. Primjeri prikupljivih metoda su potpis te prepoznavanje i termogram lica. Skeniranje mrežnice oka primjer je slabo prikupljive metode.
5. Učinkovitost se odnosi na točnost i brzinu biometrijske metode.
6. Prihvatljivost označava u kojoj su mjeri korisnici spremni dozvoliti sustavu da prikuplja njihove biometrijske karakteristike. Sustavi poput skeniranja mrežnice zahtijevaju prodor laserskog snopa u oko korisnika što u je velikom broju slučajeva prenametljivo i doprinosi nepopularnosti metode.
7. Mogućnost zaobilaženja pokazuje koliko je lako zavarati sustav korištenjem prevarantskih metoda. Automatizirani sustavi bez nadzora operatera podložniji su.
8. Troškovi biometrijskih sustava bitan su faktor usporedbe. Dijele se na inicijalni trošak za potrebnu hardversku i softversku opremu, troškove održavanja i licenciranja.

Zaštita podataka šifriranjem

Kriptografija je znanost

* koja koristi matematiku i matematičke metode za kriptiranje i dekriptiranje podataka
* o načinima pretvorbe informacija u neshvatljiv oblik, razumljiv samo primatelju koji ima određeno znanje

Sama enkripcija se sastoji od toga da se izvorni tekst (ili bilo kakva druga informacija) sakrije tj. prikaže na nerazumljiv način svima osim osobama koje poznaju dekripcijski ključ.

* u engl. području šifriranje se naziva kodiranje (Coding, Codifying) a šifra kod (Code)

Kriptologija se dijeli na dva područja:

1. kriptografija - kako sakriti neki tekst (krypto – skrivam, grafo -pišem)
2. kriptoanaliza - kako razotkriti neki tekst.

Povijest kriptografije

* Egipćani prije više od 4000 godina koristili kriptografske sustave za zaštitu informacija.
* Kriptografija se počela ubrzano razvijat tijekom 2. svjetskog rata.
- Enigma to je bio mehanički stroj za kriptiranje koji je pomoću rotora i mehaničkih kontakata šifrirao poruke te omogućava njemcima da tajno razgovaraju sa svojim podmornicama.
Collossus – stroj koji je dešifrirao poruke napravljene pomoću Enigme.
* Početkom 60-ih sa razvojem računala došlo je do sve većih zahtjeva za zaštitom informacija a time i do razvoja kriptografije.
* U zadnjih 20-ak godina desila se prava eksplozija u razvoju kriptografije
* Danas je situacija bitno drugačija. Postoji puno sustava, što besplatnih koji omogućavaju vrlo visoki nivo kriptiranja svakome tko želi. Doduše u nekim državama i danas postoje zakoni o ograničenju korištenja kriptografskih alata, ali sve je to uzaludno kada se na internetu mogu naći gotovo sve implementacije kriptografskih metoda.

Osnovni ciljevi kriptografije su:

* tajnost podataka: da podacima mogu pristupiti samo oni koji smiju
* integritet podataka: da se otkrije neovlaštena promjena podataka
* provjera identiteta: dokazivanje da su stranke u komunikaciji zaista one koje tvrde da jesu
* neosporivost: onemogućava sudioniku komunikacije da zaniječe svoje prethodne poruke

Postoji par osnovnih metoda enkripcije.

Simetrični ključ- za kriptiranje i dekriptiranje koristi se jedan ključ.

Metoda javnog ključa koristi par ključeva za enkripciju:

* Javni ključ: koji služi za kriptiranje podataka
* Tajni ključ: koji služi za dekripciju

Javni ključ objavimo svima koji žele sigurno komunicirati sa nama. Svatko sa kopijom javnog ključa može kriptirati podatke koje jedino mi možemo dekriptirati pomoću našeg tajnog ključa. To nam omogućuje da komuniciramo i sa ljudima koje i ne poznajemo. Nemoguće je iz javnog ključa nikakvom metodom dobiti tajni ključ. Neki od primjera kriptiranja javnim ključem su: RSA, DSA, Egamal ...

Digitalni potpis omogućuje primatelju informacije da utvrdi autentičnost porijekla same informacije i njenu izvornost (da nije bila mijenjana tokom puta). Digitalni potpis ima istu svrhu kao i potpis rukom samo što je digitalni potpis gotovo nemoguće krivotvoriti.

Sve kriptirane poruke imaju i potencijalne napadače. Postoje dvije vrste napada:
- pasivni - pasivni napadač promatra tok podataka i samo može narušiti privatnost
- aktivni - aktivni napadač želi izmijeniti sadržaj razmjenjivanih informacija.

Tekst koji se kodira naziva se poruka, a kodirani tekst nazivamo kriptogram.

Primjer monoabecednog kodiranja.

 Cezarov kod ili šifra - da se svako slovo abecede zamjene slovima abecede koja su pomaknuta za tri mjesta.

# KAKO ZAŠTITITI SVOJE RAČUNALO

Opasnosti rada na mreži:

* Opasnost neovlaštenog upada u računalo
* Neovlaštenog korištenja podataka
* Uništavanja programa

Def. Virus je mali program (nekoliko Kb) kojemu je svrha pravljenje štete na računalu. Ubrajaju se u grupu tzv. zlonamjernih štetnih (malware) programa (Malicius Software).

Virus je program ili dio programskog koda koji se pridružuje programima u računalu i čini štetu na datotekama, programima i hardveru ili pogoršava karakteristike rada na računalu.

* Ne širi se bez djelovanja čovjeka
* Širi se preko podataka s prenosivih medija, ili otvaranjem privitaka koji su došli s primljenom poštom.

Svaki virus radi neku štetu na računalu bilo da:

* Zauzima prostor na disku ili memoriji - čime se usporava rad na računalu ili usporava veza kada ste na Internetu
* Izbaci neku poruku
* Briše podatke na računalu ili ih mijenja
* Šalje podatke s vašeg računala na neku slučajnu e-mail adresu

Virusa ima na tisuće, a njihovih varijanti na stotine tisuća.

Vrste virusa:

* Crvi
* Trojanski konj
* Stopljena prijetnja – kombinacija nekih ili svih zlonamjernih programa
* Backdor - je program koji je instaliran od strane virusa, crva ili trojanskog konja i koji trećim osobama omogućava nesmetan i neovlašten pristup računalu bez znanja vlasnika. - koristi slabosti operativnog sustava ili zaštite ( firewalla i antivirusnog programa ).
* Spyware- u najbezazlenijem slučaju prikazuju neželjene reklame i oglase dok u najgorem slučaju mogu slati osobne informacije o korisniku, poput zaporki i brojeva kreditnih kartica trećim osobama.

Dialeri -Naziv ovog oblika zlonamjernog koda dolazi od engleske riječi 'dial', što u danom kontekstu znači birati broj (na telefonu). Dialeri nam često dolaze jednakim putevima kao i trojanski konji. Njihova je zadaća u trenutku aktiviranja prekinuti postojeću vezu s Internetom i uz pomoć modema birati broj u nekoj dalekoj zemlji kako bi ostvarili dobit autoru kroz astronomske cijene poziva.

* ROOTKIT - je program koji služi za prikrivanje aktivnosti drugih malicioznih programa
* Hoax – lažna obavijest o virusu

Phishing – je niz radnji i pokušaja da se dođe do osobnih podataka i osjetljivih informacije koje se kasnije mogu poslati drugome ili zloupotrijebiti

Kako ću znati da me virus napao? (str, 36)

Osnovna zaštita od virusa provodi se antivirusnim softverom koji se mora stalno nadograđivati.

Antivirusni programi su besplatni( Antivir i AVG) ili komercijalni (Norton, McAfee, Sophos, Kaspersky).