Doc.dr. sc. Marija Boban[1]
Mirjana Perišić, mag. forenzike[2]

BIOMETRIJA U SUSTAVU SIGURNOSTI, ZAŠTITE I NADZORA INFORMACIJSKIH SUSTAVA

Pregledni rad / Review
UDK 004.93:004.056

Poticanje integracije u globalnom društvu u nastajanju, gospodarsko i kulturno povezivanje s ostatkom svijeta, svekoliki razvoj stvara nove mogućnosti kao i nove rizike. S jedne strane brišu se granice i povećava se mobilnost ljudi, protok roba, kapitala, te druge gospodarske aktivnosti. Brz razvoj digitalne, informacijske i komunikacijske tehnologije, sveprisutnost Interneta, postali su naša svakodnevnica i njihovog utjecaja često nismo ni svjesni. Rastuća povezanost infrastruktura prometnih, energetskih, zdravstvenih i drugih područja s informacijskim tehnologijama, povećava ranjivost modernog društva. Koliko god tehnologija svijet učinila naprednijim i sigurnijim, otvorila je vrata nekim novim dimenzijama kriminala. Kompleksnost stvaranja sigurnosnog okruženja iznimno raste. Bez pouzdanih sustava osiguranja osoba i imovine, ugrožene su brojne svakodnevne aktivnosti. Značajan čimbenik pri postizanju sigurnosti je identifikacija osobe. Do sada se provjera identiteta vršila isključivo pomoću sigurnosnih zaporki, kartica, pin kodova i vlastoručnih potpisa, no to u današnje vrijeme postaje sve nepouzdanje i ograničavajuće. Biometrija svakodnevno postaje sve češći oblik autentifikacije u različitim sferama života.

Svaka biometrijska metoda ima svoje prednosti i nedostatke, a sam izbor ovisi o primjeni. No unatoč dostignućima biometrije, treba imati na umu da je ona samo jedan od alata koji se može koristi u sustavu identifikacije te da ne postoji savršena metoda koja ne podliježe pogreškama. Posebno je važno naglasiti da u pozadini stoji robusna tehnička infrastruktura kojom se vrši analiza, pohrana podataka u bazu, uspoređivanje, daljnja distribucija i da pristup takvim sustavima zahtijeva postavljanje posebni sigurnosnih protokola. Pitanja čuvanja pohranjenih biometrijskih podatka, pitanja sigurnosti i distribucije podataka te tko sve će imati pravo koristiti podatke su pitanja na koje zajednički trebaju dati odgovor čelnici država unije. Postojeća zakonska regulativa je dobar temelj za uređenje navedenih pitanja.

***Ključne riječi**: informacijski sustavi, informacijska sigurnost, sigurnosni rizik, prevencija rizika, zakonska regulativa, biometrija, biometrijski sustavi.*

1. Uvod

Globalizacija mijenja svijet i donosi posve novu dimenziju u svim sferama društva političkim, ekonomskim, sociološkim, financijskim i tehnološkim. Poticanje integracije u globalnom društvu u nastajanju, gospodarsko i kulturno povezivanje s ostatkom svijeta, svekoliki razvoj

[1] Pravni fakultet Sveučilišta u Splitu
[2] Visoka poslovna škola Minerva, Dugopolje

stvara nove mogućnosti kao i nove rizike. S jedne strane brišu se granice i povećava se mobilnost ljudi, protok roba, usluga, kapitala, te druge gospodarske aktivnosti. Šire se ideje i informacije preko Interneta i putem ostalih medija diljem svijeta, osvješćuje se kulturološka raznolikost, šire se vidici i svijest o ljudskim pravima i demokraciji. Tehnološke inovacije i know how dostupnije su no ikada, nudeći nove prilike i napredak. S druge strane globalizacija donosi i nove opasnosti. Rastuća povezanost infrastruktura prometnih, energetskih, zdravstvenih i drugih područja s informacijskim tehnologijama, povećava ranjivost modernog društva.

Brz razvoj digitalne, informacijske i komunikacijske tehnologije, sveprisutnost Interneta, postali su naša svakodnevnica i njihovog utjecaja često nismo ni svjesni. O nama se svakodnevno prikupljaju podaci poradi identifikacije: u bankama, trgovinama, zdravstvenim ustanovama, školama, fakultetima, društvenim mrežama. Mnogi ni ne razmišljaju o načinu uporabe prikupljenih podataka, koliko su podaci o nama sigurni, koliko i tko se brine o zaštiti naših identiteta, tko je sve ovlašten za pristupanje našim podacima, kolika je mogućnost zlouporabe podataka.

Koliko god tehnologija svijet učinila naprednijim i sigurnijim, toliko je na drugu stranu ostavila mogućnost većoj dostupnosti podacima, zadiranju u privatnost osobe, zlouporabi podataka. Otvorila je vrata nekim novim dimenzijama kriminala, jer se i počinitelji sve češće koriste sofisticiranim tehnikama i metodama. Kompleksnost stvaranja sigurnosnog okruženja iznimno raste a, tu biometrijske metode u sustavu zaštite, imaju ključnu ulogu. Danas se biometrijske značajke uglavnom opisuju kroz slijedeće osobine: jedinstvenost, stalnost, univerzalnost, prihvatljivost, prikupljivost. Osim navedenih značajki, pri evaluaciji biometrijskih metoda potrebno je voditi računa o svrsi sustava, o troškovima analize biometrijskih značajki i o cijeni sustava. Tehnologija i sigurnost kroz godine se u pravilu sustižu ciklički (nastoje ići u korak) – napredak neke tehnološke ili industrijske grane dođe do kritične točke u kojoj razina sigurnosti opadne, nakon čega se daljnji razvojni napori ulažu upravo u povećanje njezine sigurnosti i pouzdanosti.

2. Sigurnost informacijskih sustava

Kako bismo analizirali sigurnost i nadzor infromacijskih sustava i ulogu biometrije nužno je prvenstveno pojmovno definirati informacijski sustav (eng. *Information System* – IS) definira se kao strukturirani sustav u kojem su međusobno povezani hardveri, softveri, telekomunikacijske mreže a, ljudi ih grade i njima upravljaju u svrhu prikupljanja podataka, njihove pohrana, obrade i daljnje distribucije, te da isti budu dostupni ovlaštenim korisnicima. [27] Informacijski sustav dio je gotovo svakog poslovnog sustava, neovisno koju vrstu poslovnih procesa podržava ili veličini organizacije u kojoj funkcionira, IS je ključni element poslovanja. Svakako da je njegova povećana uloga i važnost popraćena galopirajućim rastom i primjenom informacijske komunikacijske tehnologije (eng. *Information and Communication Technology* – ICT). Cilj IS-a je prikupljanje, obrada, pohrana, čuvanje i distribucija informacija potrebnih pri izvođenju poslovnih procesa i upravljanju poslovnim sustavom. Uobičajeni su dijelovi IS-a sustav za obradu transakcija, upravljački izvještajni sustav, sustav za potporu i odlučivanje i sustav uredskog poslovanja. IS djeluje unutar poslovnom sustava, a na taj način omogućuje mu da je u interakciji sa internom i eksternom okolinom organizacije.[7]

Djelovanje IS-a upotpunjuje se primjenom ICT i s njima povezanim potrebnim programima, procedurama, uputama, algoritmima i znanjem kojima se informacijske tehnologije pokreću, s ciljem izvršavanja poslovnih zadataka i ciljeva.

Ljudi su sastavni dio IS-a (eng. *lifeware*) koji primjenom znanja formaliziraju poslovno okruženje u podatke, procedure, informacije, algoritme, te usklađuju primjenu ICT-a i programske podrške, ispunjavaju poslovne zadatke i funkcije (kao što su dostavljanje i čuvanje podataka neophodnih za odlučivanje, održavanje procesa te razvoj i neprekidnost poslovanja). U IS-u se opisuje, preslikava poslovni sustav, drugim riječima, predstavlja njegov informacijski model. Svi elementi poslovnog sustava kao što su podaci, aktivnosti, zadaci, funkcije, izvršitelji, procedure, preslikavaju se na model IS-a gdje ih dijelimo na:[20]

- modele podataka – definira podatke koji nastaju ili se koriste u poslovnom sustavu
- modele procesa – definira procese ili funkcije koje se odvijaju u poslovnom sustavu
- model izvršitelja – definira one elemente koji obavljaju funkciju u poslovnom sustavu

Značajno je istaknuti i temeljne aktivnosti poslovnog sustava:

1. izvršavanje poslovnih procesa, pri tom se misli na osnovnu djelatnost nekog poslovnog sustava, (neovisno o djelatnosti i veličini organizacije), odnosno sve one poslove koji se u njemu obavljaju (npr. nabava sirovine i energije, proizvodnja, daljnji plasman proizvoda, razne marketinške i financijske transakcije itd);
2. upravljanje poslovnim sustavom, pri tom se misli na to kako svaki poslovni sustav (neovisno radi li se o državnim tijelima ili pravnoj osobi) nastoji izgraditi dobar informacijski sustav koji će dati podlogu za brzo i kvalitetno odlučivanje.

Navedene aktivnosti podupire neka vrsta informacijskog sustava. Efikasnost i uopće funkcioniranje nekih poslovnih procesa bili bi nezamislivi bez korištenja informacijsko komunikacijske tehnologije. Kako je već navedeno, IS se definira kao dio tj. preslika poslovnog sustava a čine ga potrebna infrastruktura, koju čine svi potrebni fizički uređaji i oprema, kojim upravlja čovjek s ciljem što efikasnijeg izvršavanja poslovnih ciljeva. IS-e razlikujemo prema njihovoj kompleksnosti: na jednostavne, složene i inteligentne IS-e. Prema njihovom opsegu postoje: IS-e na razini društva, republike, županije, regije itd. Prema području primjene: IS-e odlučivanja, nabave, prodaje, itd.

2.1. Informacijska sigurnost kao integralni dio sigurnosti informacijskih sustava

Proces informacijske sigurnosti sastoji se od propisane sigurnosne politike koja obuhvaća niz mjera i metoda implementiranih u obliku organizacijskih i tehničkih kontrola u poslovne procese, određene pravne osobe ili državnog tijela.

Pojam informacijske sigurnosti definira se kao stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda. [31] Pod pojmom sigurnosti podrazumijeva se zaštita informacijskog sustava od velikog broja prijetnji, kako bi se osigurao poslovni kontinuitet, smanjio rizik na prihvatljivu razinu. Svakodnevno se organizacije suočavaju s brojnim sigurnosnim prijetnjama poput računalnih prijevara, računalnog hakiranja sustava, špijunaže, zloćudnog koda pa do onih iza-

zvanih elementarnim nepogodama kao što su potresi, poplave itd. Štete mogu biti velikih razmjera, a informacijska sigurnost jednako je važna javnim i privatnim organizacijama. Mjere kojima se štiti ovakav oblik sigurnosti opća su pravila zaštite podataka koji se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini. Sami standardi informacijske sigurnosti su organizacijske i tehničke procedure te rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti. Zaštita podrazumijeva provođenje mjera poradi osiguranja sigurnosti IS-a.

Nadzor informacijskog sustava može se definirati kao niz poduzetih radnji u sustavu provjere učinkovitosti sustava zaštite. Informacijska sigurnost se postiže postavljanjem, implementacijom i primjenom odgovarajućih kontrola, koje se odnose na sigurnosnu politiku, procese, procedure, strukturu organizacije i funkciju sklopovske i programske opreme. U tom kontekstu, politika informacijske sigurnosti, predstavlja skup dokumenta kojima se utvrđuju mjere i standardi informacijske sigurnosti koje je potrebno primijeniti kako bi se osigurala sigurnost sustava, zaštitila povjerljivosti, cjelovitosti i raspoloživosti podataka te ujedno i raspoloživosti i cjelovitosti informacijskih sustava u kojima se ti podaci obrađuju, pohranjuju ili prenose.

Dokumenti sigurnosne politike predstavljaju izjavu ili očitovanje odgovornih osoba (uprave tvrtke/čelnici državnih tijela) o uvjerenju, ciljevima i razlozima te općenitim načinima kako doći do željenih postignuća u području informacijske sigurnosti, i to u obliku kratkog koncicznog dokumenta na općenitoj razini, bez specifičnosti i detaljnih opisa. Dokumenti sigurnosne politike predstavljaju hijerarhijski strukturirani skup propisa koje se, pored opisanog krovnog dokumenta, uobičajeno sastoji i od razine standarda (obvezujućih zahtijeva), razine procedura (obvezujući postupci) te od razine smjernica ili naputaka (preporučeni načini realizacije standarda i procedura). Primjenom odgovarajućih sigurnosnih standarda osigurava se sigurnost unutar različitih poslovnih sustava i korisničkih okruženja. Pod pojmom informacijske sigurnosti nužno je promatrati širu sliku, društvo i informacijski prostor u cjelini, uvažavajući i usklađujući razlike i potrebe informacijske sigurnosti u različitim sektorima društva.

2.2. Područja informacijske sigurnosti

Sukladno ZIS-u područja informacijske sigurnosti predstavljaju podjelu informacijske sigurnosti na pet područja s ciljem sustavne i učinkovite realizacije donošenja, primjene i nadzora mjera i standarda informacijske sigurnosti: sigurnosna provjera, fizička sigurnost, sigurnost podatka, sigurnost informacijskog sustava i sigurnost poslovne suradnje.

2.2.1. Sigurnosna provjera

Sigurnosna provjera je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti koji se primjenjuju na osobe koje imaju pristup klasificiranim podacima. Osobe trebaju biti ovlaštene te su obvezne ishoditi uvjerenje o sigurnosnoj provjeri (cetifikat). Sukladno Zakonu pravne osobe koji koriste klasificirane podatke stupnja tajnosti „Povjerljivo", "Tajno" i „Vrlo tajno", dužne su ustrojiti: [31] popis osoba koje imaju pristup klasificiranim podacima i registar zaprimljenih certifikata s rokovima važenja certifikata.

2.2.2. Fizička sigurnost

Sukladno ZIS-u, fizička sigurnost definira se kao područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti za zaštitu objekta, prostora i uređaja u kojem se nalaze klasificirani podaci. Također, tijela i pravne osobe koje rukuju klasificiranim podacima stupnja tajnosti „Povjerljivo", "Tajno" i „Vrlo tajno", dužne su izvršiti kategorizaciju objekata i prostora na sigurnosne zone, propisane mjerama i standardima informacijske sigurnosti. [31]

2.2.3. Sigurnost podataka

Sigurnost podataka je područje informacijske sigurnosti za koje se utvrđuju mjere i standardi informacijske sigurnosti koje se primjenjuju kao opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka. Prema ZIS-u, tijela s javnim ovlastima i pravne osobe koje koriste klasificirane i neklasificirane podatke u svom djelokrugu, dužni su primijeniti procedure o postupanju s klasificiranim i neklasificiranim podacima, o sadržaju i načinu vođenja evidencije o izvršenim uvidima u klasificirane podatke te nadzoru sigurnosti podataka, propisanim mjerama i standardima informacijske sigurnosti. [31]

2.2.4. Sigurnosna dokumentacija informacijskog sustava

Sigurnosna dokumentacija informacijskog sustava obvezujući je dokument za vlasnika informacijskog sustava koji se definiraju mjere informacijske sigurnosti i odgovornosti unutar informacijskog sustava. Sigurnosnu dokumentaciju čine: a) dokumentacija sigurnosne procjene rizika informacijskog sustava, b) specifikacija sigurnosnih zahtjeva sustava, c) specifikacija sigurnosnih zahtjeva povezivanja sustava i d) sigurnosne operativne procedure.

Struktura i elementi sigurnosne dokumentacije propisane su odredbama ZSIS-a i objavljeni na internet stranicama ZSIS-a.

2.2.5. Sigurnost poslovne suradnje

Sigurnost poslovne suradnje je područje informacijske sigurnosti u kojem se primjenjuju propisane mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranom dokumentacijom koji obvezuju i pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima. [31]

2.3. Prijetnje informacijskom sustavu

Sigurnost informacijskog sustava može biti ugrožena na više načina a mogu se podijeliti na slijedeći način: [27] djelovanje ljudi (nenamjerna i namjerna prijetnja), oprema (mehanička oštećenja, prestanak napajanja opreme) i prirodne nepogode (potresi, poplave, požari).

2.3.1. Kategorije napada

U osnovi, napadi su sve akcije usmjerene na ugrožavane sigurnosti informacijskog sustava, pod tim se misli na informacije, računalni sustava i samu mrežu. Postoje različite vrst napada, ali generalno se mogu podijeliti na: [20] presijecanje, prekidanje komunikacijskog kanala (eng. i*nterruption*), presretanja informacija u komunikacijskom kanalu (eng. *interception*), izmjena informacija (eng. *modificiation*) i proizvodnja (eng. *fabrication*).

Kad se govori o definiranju sigurnosnih zahtijeva obavezno se uzimaju u obzir tri najvažnije kategorije: procjena rizika, propisani zakoni, te skup ciljeva, načela i poslovnih zahtijeva organizacije.

2.4. Sigurnosni rizik i procjena rizika

Prilikom procjene rizika uzima se u obzir poslovna strategija organizacije i njezini ciljevi. Kroz samu procjenu rizika identificiraju se moguće prijetnje imovini organizacije i stupanj ranjivosti. Također, određuje se i vjerojatnost pojava prijetnji i njihov utjecaj na rad organizacije te eventualnu procjenu štete. [24] Sigurnosni rizik definira se kao mogućnost realizacije nekog neželjenog događaja. Neželjeni događaj može utjecati na:

– povjerljivost (eng. *confidentiality*) se odnosi na zaštitu određenih sadržaja, od bilo kakvog namjernog ili nenamjernog otkrivanja neovlaštenim osobama;
– integriteta (eng. *integrity*) - mora osigurati konzistentnost informacija i onemogućiti bilo kakve neovlaštene promjene sadržaja;
– raspoloživost (eng. *availability*) informacijskih resursa podrazumijeva da su sve relevantne informacije, u za to vremenski prihvatljivom terminu, raspoložive odgovarajućim (ovlaštenim) subjektima

Pod pojmom „ranjivosti sustava" podrazumijevaju se svi propusti i slabosti sustava sigurnosti koji omogućuju provođenje eventualnih nedopuštenih aktivnosti. Ranjivosti sustava najčešće se povezuju s propustima programskog koda, no mogući su i mnogi drugi propusti kao što su propusti u dizajnu samog sustava, propusti u implementaciji i održavanju sustava, neprikladan odabir tehnologije i alata itd. Bez adekvatno provedene analize ranjivosti, gotovo je nemoguće odrediti sigurnosni rizik.

2.4.1. Upravljanje sustavima informacijske sigurnosti

Sustav upravljanja informacijskom sigurnošću (engl. *Information Security Management System* – ISMS) dio je sveukupnog sustava upravljanja, utemeljen na pristupu upravljanju rizicima, s ciljem uspostavljanja, provođenja, praćenja, revidiranja, održavanja i unaprjeđivanja informacijske sigurnosti. [24] Temelj ISMS-a je upravljanje rizikom.

Upravljanje rizikom (eng. *Risk Managment*) je relativno nova disciplina u području informacijskih sustava, koja je proizašla iz potrebe standardizacije i formalizacijom postupka vezanih uz upravljanje sigurnošću. Proces upravljanja rizicima sastoji se od tri faze :[24] procjena rizika (eng. *Risk Assessment*), umanjivanje rizika (eng. *Risk Mitigation*) i ispitivanje i analiza (eng. *Evaluation and Assessment*).

Upravljanje rizicima, kako je već navedeno, kao proces predstavlja identifikaciju onih čimbenika koji mogu negativno utjecati na povjerljivost, integritet i raspoloživost informacijskih resursa, kao i njihova analiza u smislu vrednovanja pojedinih resursa i troškova njihove zaštite. Kao krajnji korak procesa je poduzimanje odgovarajućih zaštitnih mjera koje će identificirani sigurnosni rizik svesti na prihvatljivu razinu, u skladu sa poslovnim ciljevima organizacije.

Najvažniji i prvi korak kod upravljanja rizicima je identifikacija, tj. klasifikacija informacijskih resursa. Pod pojmom informacijski resursi podrazumijevaju se oni resursi koje organizacija koristi u svrhu ostvarivanja svojih poslovnih ciljeva, to su sklopovlje, programi, mreže, ljudski resursi i podatci. Neadekvatna klasifikacija resursa može cijeli proces odvesti u krivom smjeru, čime se gubi njegov značaj i smisao. Odabir kontrola ovisi prije svega odluka ovisi o top menadžmentu organizacije o dokumentima sigurnosne politike te o predviđenim financijskim sredstvima tj budžetom. Upravljanje informacijskom sigurnošću zahtijeva aktivno učešće svih djelatnika organizacije.

Osim osnovnih zahtjeva koje proces upravljanja sigurnošću sustava mora osigurati, treba naglasiti i pojmove koji su usko vezani uz implementaciju sigurnosnih kontrola, a to su: identifikacija - podrazumijeva predstavljanje korisnika unutar sustava, autentifikacija - podrazumijeva proces dokazivanja identiteta korisnika, autorizacija - proces koji se korisniku odobrava ili zabranjuje pristup odnosno korištenje određenih resursa unutar sustava, zaštita i mogućnost praćenja.

2.5. Pravno uređenje informacijske sigurnosti RH

Smisao pravnog uređenja informacijske sigurnosti je postizanje adekvatnih sigurnosnih kriterija na razini države. Procesom uvođenja informacijske sigurnosti, između ostaloga, osuvremenjen je sustav sigurnosne klasifikacije dokumenata i ujednačen način postupanja s podacima, također su razgraničeni podaci u vlasništvu državne uprave od javnih podataka, te uvedene jasne i transparentne procedure objavljivanja u tijelima državne vlasti. Temelj postojećem zakonodavnom okviru po pitanjima informacijske sigurnosti dao je Nacionalni program informacijske sigurnosti predstavljen 2005. godine. Nacionalni program dao je okvir za niz aktivnosti usmjerenih zakonskom reguliranju pitanja informacijske sigurnosti te definirao i nadležnosti pojedinih tijela po pojedinim pitanjima. Mnoga od tih rješenja ugrađena su i u postojeći Zakon o informacijskoj sigurnosti. [31]

Mjere informacijske sigurnosti propisuju se uredbom koju donosi Vlada Republike Hrvatske, a standardi za provedbu mjera propisuju se pravilnicima koje donose čelnici središnjih državnih tijela za informacijsku sigurnost. Vlada donosi uredbe i za primjenu odredaba Zakona o obradi posebnih kategorija osobnih podataka i odredaba o uspostavi evidencije zbirki osobnih podataka. Uredbama se propisuje načini pohranjivanja i posebne mjere tehničke zaštite posebnih kategorija osobnih podataka te način vođenja evidencije koja sadrži temeljne informacije o zbirci osobnih podataka.

Postojeća zakonska regulativa koja regulira pitanja informacijske sigurnosti u RH: Zakon o informacijskoj sigurnosti [31], Zakon o zaštiti osobnih podataka [32], Zakon o pravu na pristup informacijama [35], Zakon o sigurnosno – obavještajnom sustavu RH [33], Zakon o tajnosti podataka [34], Zakon o sigurnosnim provjerama [36], Zakon o elektroničkoj ispravi

[37], Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima [28], Uredba o mjerama informacijske sigurnosti [29], Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima [30].

2.5.1. Središnja tijela RH za informacijsku sigurnost

Sukladno Zakonu o informacijskoj sigurnosti, središnje tijelo nadležno za pitanja informacijske sigurnosti je Ured vijeća za nacionalnu sigurnost dok za tehnička pitanja informacijske sigurnosti je nadležan Zavod za sigurnost informacijskih sustava – dalje ZSIS. Za poslove prevencije i otklanjanja problema vezanih uz sigurnost računalnih mreža u Republici Hrvatskoj nadležan je CARNet CERT (www.cert.hr), zasebna ustrojstvena jedinica pri Hrvatskoj akademskoj i istraživačkoj mreži CARNet. [31] Nadzor nad zaštitom i obradom osobnih podataka vrši Agencija za zaštitu osobnih podataka kao neovisno i samostalno tijelo.

1) Ured Vijeća za nacionalnu sigurnost je središnje državno tijelo za informacijsku sigurnost koje koordinira i usklađuje donošenje i primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj i u razmjeni klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija. Njegova funkcija temelji se na trajnom usklađivanju propisanih mjera i standarda informacijske sigurnosti u Republici Hrvatskoj s međunarodnim standardima i preporukama informacijske sigurnosti te sudjeluje u nacionalnoj normizaciji područja informacijske sigurnosti. Također, surađuje s mjerodavnim institucijama stranih zemalja i organizacija u području informacijske sigurnosti te koordinira međunarodnu suradnju ostalih tijela i pravnih osoba. [31]
2) Zavod za sigurnost informacijskih sustava – dalje ZSIS, predstavlja središnje državno tijelo za tehnička područja sigurnosti informacijskih sustava u tijelima i pravnim osobama. [31] Funkcija ZSIS-a trajno je usklađivanje standarda tehničkih područja sigurnosti informacijskih sustava u RH s međunarodnim standardima i preporukama te sudjeluje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava. ZSIS je također nadležan za upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka između državnih tijela i stranih država i organizacija te koordinaciju prevencije i otklanjanja problema vezanih uz sigurnost računalnih mreža u državnim tijelima. ZSIS obavlja i poslove sigurnosne akreditacije informacijskih sustava u suradnji s Uredom Vijeća za nacionalnu sigurnost.
3) Nacionalni CERT, zasebna je ustrojstvena jedinica koja se ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (CARNet). CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u RH. Funkcija CERT-a je usklađivanje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u RH, ili u drugim zemljama i organizacijama, kad su povezani s RH. CERT usklađuje i rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u RH te određuje pravila i načine zajedničkog rada.[31]
4) Agencija za zaštitu osobnih podataka kao neovisno i samostalno tijelo, ima svojstvo pravne osobe i za svoj rad je odgovorna Hrvatskom saboru. Agencija ima nadzorne ovlasti, ovlasti intervencije i savjetodavnu ulogu.

2.5.2. Primjena pravila zaštite podataka Europske unije i njenih članica

Europska unija je utemeljena je na načelima slobode, demokracije, poštivanja ljudskih prava i temeljnih sloboda te vladavine prava, načela koja su zajednička svim državama članice. Direktivom Europskog parlamenta i Vijeća Europske zajednice o zaštiti pojedinaca u svezi s obradom osobnih podataka i slobodnim kretanjem tih podataka [8] osnažuju se i proširuju načela zaštite prava i sloboda pojedinca, posebno prava na privatnost koje su sadržane u Konvencijom 108, usvojenoj od strane Vijeća Europe. [41]

Direktiva ima za cilj ukloniti prepreke na protok osobnih podataka koji zahtijevaju visoku razinu zaštite temeljnih prava (posebno prava na privatnost) u državama članicama te usklađivanje različitih zakonskih rješenja o zaštiti podataka u državama članicama EU-a. Ujedno predstavlja pravnu podlogu za biometrijske tehnologije. Načela ugrađena u Direktive svaka zemlja članice morala je uključiti u nacionalne zakone. RH-a kao punopravna članica je također uskladila svoje zakone pa je tako Zakon o zašiti osobnih podataka temeljni dokument koji se regulira način i uvjeti obrade osobnih podatka, obrada posebnih kategorija osobnih podataka, obvezu obavještavanja ispitanika, povjeravanje poslova, iznošenje osobnih podataka iz RH-e. Nadalje, zakonom se uređuje pitanje čuvanja osobnih podataka, za što su odgovorni voditelji zbirki osobnih podataka i korisnici, a, oni su ujedno zaduženi za poduzimanje tehničkih, organizacijskih i kadrovskih mjera zaštite osobnih podataka. Zakonom o pravu na pristup informacijama propisuju se uvjeti pod kojima je potrebno osigurati pravo na pristup informacijama.

2.5.3. Mjere, norme i standardi koji uređuju informacijsku sigurnost

Razlikuju se mjere i standarde informacijske sigurnosti koji se utvrđuju za klasificirane i neklasificirane podatke, sukladno stupnju tajnosti, broju, vrsti te ugrožavanju klasificiranih i neklasificiranih podataka na određenoj lokaciji. Sukladno ZIS-u mjere i standardi informacijske sigurnosti definiraju se kao niz mjera kojima se štiti ovakav oblik sigurnosti a predstavljaju opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini. Sami standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti. [31]

Mjere i standardi informacijske sigurnosti utvrđuju se za klasificirane i neklasificirane podatke i njima se utvrđuju minimalni kriteriji za zaštitu klasificiranih i neklasificiranih podataka u tijelima i pravnim osobama. [18] Mjere i standardi informacijske sigurnosti utvrđuju se sukladno stupnju tajnosti, broju, vrsti te ugrozama klasificiranih i neklasificiranih podataka na određenoj lokaciji uz obvezu trajnog provođenja sigurnosne prosudbe ugroza za klasificirane podatke stupnja tajnosti „Povjerljivo", „Tajno" i „Vrlo tajno". [31]

ZIS nadalje definira mjere i standarde informacijske sigurnosti na način da obuhvaćaju: nadzor pristupa i postupanja s klasificiranim podacima, postupanje prilikom neovlaštenog otkrivanja i gubitka klasificiranih podataka, planiranje mjera prilikom izvanrednih situacija, ustrojavanje posebnih fondova podataka za podatke klasificirane u Republici Hrvatskoj te za klasificirane podatke koje je predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje. [18] Također, mjere i standardi informacijske sigurnosti za zaštitu neklasificiranih podataka utvrđuju se u skladu s mjerama i standardima zakonom

propisanim za zaštitu osobnih podataka građana, dok se mjere i standardi informacijske sigurnosti za zaštitu stupnja tajnosti „Ograničeno" utvrđuju uz prethodnu provjeru primjene propisanih mjera i standarda za neklasificirane podatke i primjenu mjera i standarda propisanih za stupanj tajnosti „Ograničeno". [31]

2.5.4. Međunarodna udruga za normizaciju

Međunarodna udruga za normizaciju (eng. *International Standards Organization* - ISO) i Međunarodno elektrotehničko povjerenstvo (eng. *International Electrotechnical Commission* – IEC) zajedno čine sustav za međunarodnu normizaciju i standardizaciju. Svjetsko je udruženje nacionalnih tijela za normizaciju, koje je službeno počelo djelovati 1947. godine, a danas okuplja 148 zemalja. Na području informacijske tehnologije, ISO i IEC su osnovali zajednički tehnički odbor (eng. *Joint Technical Committee* – JTC), ISO/IEC JTC. Glavni je zadatak tehničkog odbora priprema međunarodnih standarda.

U zahtjevima koje propisuju norme, utvrđuje korištenje procesa planiranja, provedbe, provjere i dorade (engl. Plan, Do, Check, Act – PDCA), pri uspostavi i korištenju ISMS-a.

Pri tome proces predstavlja skup međuzavisnih akcija i aktivnosti koje se provode s ciljem postizanja predodređenog skupa proizvoda, rezultata ili usluga. [21] Standard sadrži strukturirani set smjernica i specifikacija za pomoć organizacijama u razvoju sustava upravljanja informacijskom sigurnošću**.** Norme su javno objavljene specifikacije koje u kontekstu informacijske sigurnosti propisuju metodologiju za pojedine aspekte informacijske sigurnosti. Certifikat i samo certificiranje vrše ovlaštene, akreditirane kuće, sukladno propisanoj normi, a sam certifikat je potvrda da je neka organizacija definirala i aktivirala efikasne procese zaštite svih resursa informacijskog sustava te da je usklađena s propisanim dokumentima sigurnosne politike.

Za zaštitu neklasificiranih podataka, državna tijela i pravne osobe utvrđuju i primjenjuju odgovarajući skup mjera informacijske sigurnosti, sukladno normama za upravljanje informacijskom sigurnošću, HRN ISO/IEC 27001 i HRN ISO/IEC 27002. [42]

Sukladno navedenom norme za sigurnost informacijskih sustava su slijedeće: ISO/IEC 27001:2005 (eng. *Information security management systems – Requirements*), bivša norma BS 7799-2 – ovo je osnovna norma za informacijsku sigurnost, definira kako postaviti temelje za sustav upravljanja informacijskom sigurnošću u organizaciji bilo koje vrste, ISO/IEC 27002:2007 (eng. *Code of practice for information security management*), bivša norma ISO/IEC 17799) – ovo su provedbene smjernice za bilo koju od 133 preporučane mjere zaštite (kontrole) – koristi se zajedno sa normom ISO/IEC 27001, ISO/IEC 27005:2008 (eng. *Infromation security risk management*) nastala na temelju norme BS 7799-3, NIST SP 800-30 (eng. *Risk management guide for infromation technology sytems*), BS 25999-2:2007 (eng. *Specification for business continuitey management*), NIST SP 800-100 (eng. *Infromation securty handbook: Aguide for managers*), ISO/IEC 24762:2008 (eng. *Guidelines for infromation and comunications tehnology disaster recovery services*). Standardi ISO/IEC 17700 (27002:2007) i 27001 ne isključuju se međusobno, naprotiv, nadopunjavaju se.

3. Biometrijske tehnologije i njihova uloga u sigurnosti informacijskih sustava

Riječ biometrija dolazi od starogrčkog bios = „život" i metron = „mjera". Prema definiciji biometrija je znanost o postupcima za jedinstveno prepoznavanje ljudi, na temelju uspore-

đivanja jednog ili više urođenih tjelesnih obilježja, ili obilježja čovjekovog ponašanja. [6] Biometrija je kao tehnika identifikacije poznata od davnina. Stari Egipćani su vršili različita mjerenja tijela za identifikaciju, u Babilonu se otisak prsta na glinenoj pločici koristio za poslovne transakcije, a u Kini je bila u upotrebi još od XIV stoljeća. Kineski trgovci su uz pomoć tinte i papira radili otiske dlanova i stopala u svrhu razlikovanja male djece. Dok su na istoku od davnina koristili neke od metoda identifikacije i tehnike razlikovanja dviju osoba, na zapadu se tek 1883. godine bilježe prvi pokušaji biometrije.

Francuski policijski službenik i znanstvenik Alphonse Bertillon je razvio prvi antropometrijski sustav kasnije nazvan Bertillonageov sustav. Taj prvi znanstveni sustav našao je široku primjenu u identifikaciji kriminalaca i prijestupnika. Sustav se temeljio na preciznom mjerenju dimenzija tijela, dužine i širine glave te evidentiranjem osobnih obilježja osobe kao što su razne tetovaže, ožiljci i deformacije tijela.[16] Sustav Bertillon se koristio sve dok njegovi propusti u radu nisu postali očigledni. Problemi koji su se javljali, najčešće su bili vezani uz neujednačene postupke mjerenja, nedovoljnoj preciznosti kod mjerenja i velikoj promjenjivosti ljudskog tijela tijekom godina. Sustav je sužavao broj počinitelja, ali nije davao točan rezultat. Brzi razvoj tehnologije povećao je i potrebu za sigurnijim načinima identifikacije osoba a ujedno je i poboljšao metode uzimanja biometrijskih značajki. Biometrijske metode su postale puno složenije i preciznije.

3.1. Biometrijske tehnologije, utvrđivanje identiteta osobe i identifikacijska obilježja

Individualna obilježja, fizičke posebnosti ono su što nas razlikuje jedne od drugih. Identitet su sva ona nepromjenjiva obilježja koja čine određenu osobu ili predmet, životinju drugačijom. Individualnost je skup individualnih obilježja koje nas čine drugačijim od drugih. [17] Identifikacija je postupak kojim se uspoređuje podudarnost ili različitost između objekata koji se uspoređuju. Sam postupak fizičke provjere identiteta osobe, podrazumijeva sve one postupke koji se provode na način da se javne isprave ili podaci iz baze podataka uspoređuju s podacima ili izgledom osobe. [17] Postupak identifikacije i autorizacije se ograničava na: Nešto što posjedujete, nešto što znate i nešto (fizički) osobno. [27] Postupka identifikacije osobe lako se provodi u slučajevima kad se samo provjerava vjerodostojnost podataka, puno složeniji postupak je u slučajevima kada je identitet osobe nepoznat ili u slučajevima kad se radi o umrloj osobi čiji identitet nije poznat.

3.2. Pohrana, obrada i verifikacija biometrijskih podataka

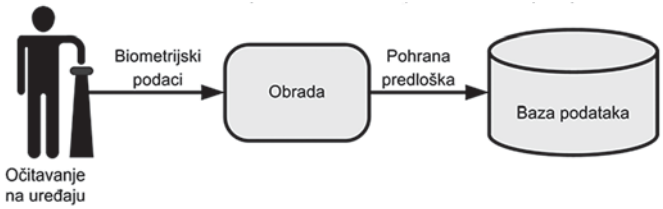
Razvojem tehnologije, posebno računalne klasične biometrijske metode doživljavaju punu afirmaciju. Suvremena biometrijska identifikacija temelji se na prepoznavanju određenih biometrijskih značajki te uspoređivanjem s pohranjenim uzorkom u podatkovnom obliku unutar baze podatka određenog sustava. Najvažniji element u procesu prepoznavanja uzoraka je digitalizacija. Prema *slici 1*, za potrebe računalne obrade, podatke dobivene skeniranjem i sl. potrebno je prevesti u digitalni format s kojim računalo može raditi. Proces u kojem se analogni signal pretvara u digitalni te prepoznaje programskom opremom. Analogni

signal se pretvara u digitalni korištenjem elektroničkog konvertera (eng. *Digital Audio – video Converter* – DAC). [6]

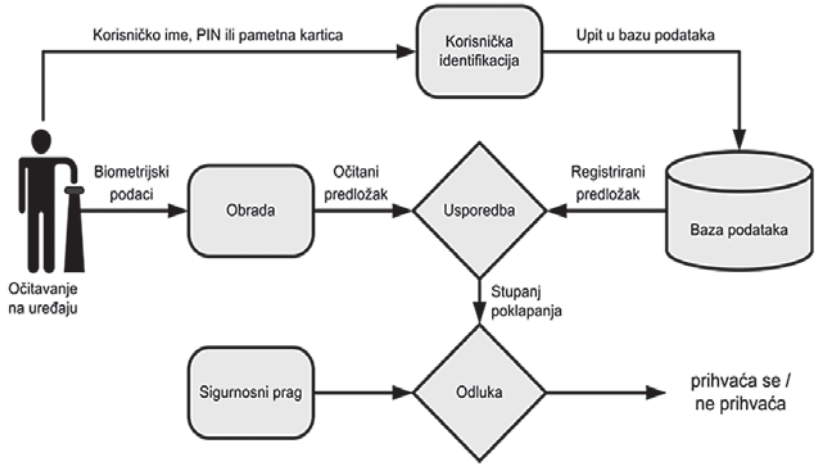
Da bi se neka osoba mogla identificirati, njezine biometrijske značajke prvo se pohranjuju u bazu podataka, zatim se analiziraju, a ako su podaci nedostatni, sustav odbija zahtjev ili se daju daljnje instrukcije za poboljšanje kvalitete. Predlošci se potom spremaju, što se može raditi na dva načina: decentralizirano (na čip karticu ili PC) i centralizirano (u bazu podataka, odnosno arhivu predložaka).

Ovisno o kvaliteti sustava biće potrebno prikupiti i pohraniti više predložaka budući da je svaki na svoj način unikatan zbog utjecaja raznih faktora tijekom registracije. [6]

Slika 1. Obrada i pohrana biometrijskih uzoraka [49]



Slika 2. Verifikacija na osnovu biometrijskih podataka [50]



Kako se vidi na *slici 2*, u sustavu se vrši verifikacija biometrijskih podataka. Nakon što je izvršen procesa registriranja biometrijskih značajki i pohrana u bazu podataka, u sustavu slijedi proces utvrđivanja identiteta osobe. Neovisno o kojim bijometrijskim značajkama se radi otisku prsta, skenu oka, mrežnice i sl. Sustav za verifikaciju zaprima biometrijski uzorak pohranjen u bazu te temeljem njega kreira probni predložak baziran na algoritmu sustava identifikacije. Nakon toga vrši se usporedba na principu 1:1 gdje sustav uspoređuje probni predložak s prije spremljenim podacima korisnika i traži podudaranje. Verifikacijski biometrijski sigurnosni sustav može sadržavati od nekoliko desetaka, pa sve do nekoliko milijuna registriranih identifikacijskih podataka. [21]

3.3. Biometrijske metode prepoznavanja

Postoje različiti načini identifikacije, autentifikacije, pin kod za kreditnu karticu, pin za mobitel, čip karticu za e-bankarstvo, svi oni na svoj način traže potvrđivanje identiteta osobe. Prepoznavanje i autentifikacije se uglavnom vrši pomoću identifikacijskih dokumenata temeljeno na sigurnosnom ključu kao standardnoj metodi. Obzirom na porast sigurnosnih zahtijeva i pad pouzdanosti standardnih metoda identifikacije, korištenjem biometrijskih metoda prepoznavanja, otklanja se mogućnost zlouporabe te umanjuju navedeni nedostaci. [14] Prema navodima stručnjaka koji se bave razvojem bimetrijskih metoda, ističu se slijedeće karakteristike biometrijskih metoda:

Prednosti biometrijskih metoda identifikacije su: biometrijski parametri su one individualne osobine koje nas definiraju, a čine različitima od drugih; biometrijske parametre je teško kopirati i krivotvoriti.

Biometrijske karakteristike su: fiziološke i ponašajne. Biometrijske metode su: kontaktne i nekontaktne.

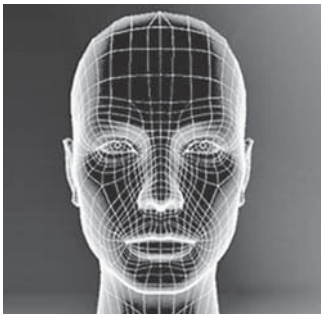
Idealna biometrijska karakteristika je: [14] univerzalnost – svaka osoba posjeduje tu karakteristiku, jedinstvenost – svaka osoba je jedinstvena, trajnost – karakteristika mora biti stalna tijekom vremena kao, npr. šarenica oka, dok se lice osobe ili glas mijenjaju starenjem osobe, prikupljivost – karakteristika se može lako izmjeriti i kvantitativno izraziti, npr.potpisi i prepoznavanje lica, prihvatljivost – karakteristika kojom se mjeri spremnost korisnika za prikupljanje biometrijskih karakteristika, izvedljivost – opisuje preciznost, brzinu i robusnost sustava za prikupljanje biometrijskih uzoraka, skalabilnost – označava fleksibilnost sustava odnosno sposobnost da se prilagodi povećim zahtjevima i troškovi – važan su faktor usporedbe. Čine ih troškovi potrebni za hardversku i softversku opremu te troškovi daljnjeg održavanja i licenciranja.

3.1.1. Fiziološke biometrijske karakteristike

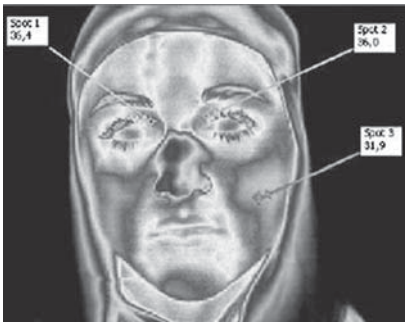
Tehnike mjerenja lica se u novije vrijeme koriste kao metode biometrijske autentifikacije, gdje računalo uspoređuje korisnikovu trenutnu dohvaćenu sliku s pohranjenom slikom. Izgled lica, poput čela, očiju, usta i nosa uvjetovan je i građom kostura glave, lica, rasporedom muskulature. Na licu (*slika 3*) je moguće mjeriti i uspoređivati preko 80 obilježja koje se ne mijenjaju tijekom godina, kao što su razmak očiju, širina nosa, dubina očnih udubljenja, jagodice, vilica, brada itd. Navedeni ključni detalji se mjere (najčešće samo njih 20-ak), te se formira numerički digitalni kod koji predstavlja lice u bazi podataka. [22]

Kad govorimo o dvodimenzionalnim algoritmima za usporedbu lica, najpoznatije su metode: algoritam svojstvenih lica, metoda kojom se uspoređuje lice osobe s unaprijed unesenim i pohranjenim slikama ljudskih lica. Druga poznata metoda je algoritam facijalne metrike, metoda kojom se analizira položaj i relativna udaljenosti između dijelova korisnikova lica (nosa, usta i očiju) te informacije o njima zapisuju se u predložak. [6] Dvodimenzionalni algoritmi se lako mogu zavarati podmetanjem slike legitimnog korisnika. Kvaliteta prepoznavanja ovisi o kutu upada svjetlosti na lice korisnika i promjeni kuta gledanja u kameru. Problem predstavlja i promjenjivost lica starenjem, različite osobe mogu imati vrlo slična lica, mijenja-

Slika 3. Tehnike mjerenja lica [51]



Slika 4. Termogram lica [52]



njem frizure, načina šminkanja, izraza lica i brade ili nošenjem naočala. Zbog nepouzdanosti i nepreciznosti dvodimenzionalne metode se malo koriste u identifikaciji. Trodimenzionalni algoritmi analiziraju i pohranjuju 3D karakteristike i veličine dijelova lica. Na taj način se izbjegavaju problemi koji karakteriziraju dvodimenzionalne metode jer svojstva trodimenzionalnog modela ne zavise o izrazu lica, trenutnom psihičkom stanju, načinu šminkanja, zakrenutosti glave i sl.

Termogram lica (*slika 4*) je relativno nova biometrijska metoda. Lice svako čovjeka prožeto je razgranatim mrežama krvnih žila. Mreža krvnih žila je jedinstvena za svakog čovjeka, čak i u slučaju kada sa radi o blizancima. Iz nje se širi toplina koje se može očitovati infracrvenom kamerom. Dobiveni uzorci su jedinstveni i za razliku od metoda prepoznavanja lica slike se mogu prikupljati neovisno o osvjetljenju okoline. Ovakvim postupkom dobiva se snimka, koja se naziva termogram, a jedinstven je za svaku osobu čak i kad se radi o blizancima. Zbog visoke točnosti i brzine obrade podataka pogodna je za identifikaciju. Iz razloga što je oprema skupa nema širu primjenu. [22]

Slika 5. Otisak prsta - papilarne linije [53]

Za otisak prsta (*slika 5*) može se reći da je najstarija i najpoznatija korištena metoda autentifikacije. Metodom analize pojedinosti analiziraju se relativni položaji individualnih karakteri-

stika otiska prsta kao što su: završeci grebena, bifurkacije (mjesta na kojima se dvije linije spajaju u jednu), uzorak izbočina i udubljenja na površini jagodice prsta, a nastaje sakupljanjem mrtvih, otvrdnulih stanica, koje se neprekidno u slojevima ljušte sa površine prsta. Oblik i formacija otiska ovise o prvotnim uvjetima razvoja embrija. Otisci prstiju su jedinstveni za svaki prst osobe, uključujući i jednojajčane blizance. Otisak prsta u primjeni je jedna od najdostupnijih i najčešće korištenih biometrijskih metoda. Postoje tri tehnike za skeniranje otisaka prstiju: optički čitač, silicijski čitač i ultrazvučni čitač.

Različitih obilježja otiska prsta je veliki broj, međutim nedostatak je mogućnost korištenja umjetno napravljenih otisaka prstiju neke osobe (pomoću voska, gela i sl). Radi zaštite od takve mogućnosti, savršeniji uređaji uz skeniranje otisaka, mjere i protok krvi. Korištenjem metode uzimanja otisaka više prstiju u procesu prepoznavanja, povećava se i sigurnost metode.

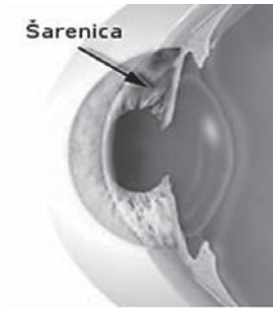
AFIS (eng. *Automated Fingerprint Identification System*) je sustav automatizirane identifikacije otisaka prstiju. Pogodan za implementaciju u kartične sustave (magnetne, smart ili optičke kartice) te se uvođenjem ove metode u postojeće sustave za identifikaciju (osobne karte, vozačke dozvole, putovnice, kreditne kartice...) povećava pouzdanost tih sustava.[19] Nekoliko država u USA provjera otiske prstiju kod prijava ljudi za socijalne povlastice (država New York ima preko 900 000 ljudi u takvom sistemu). [12]

Slika 6. Geometrija dlana [54]

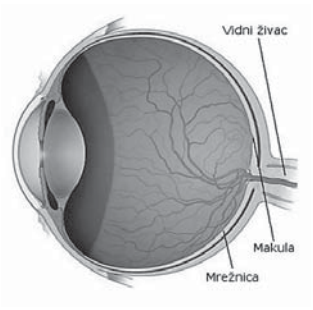
Geometrija dlana (*slika 6*) jednostavna, ne preskupa tehnika, ali i niskog praga točnosti. Često upotrebljavana na mjestima gdje je velika protočnost. Omogućava velike baze uzoraka sustavima koji zahtijevaju mali biometrički uzorak (nekoliko byte-ova). Mali troškovi i današnja elektronika omogućili su proizvodnju komercijalno dostupnog uređaja. Nedostatak je to što nakit na ruci, nedostatke dijela prstiju ili izostanak prstiju imaju veliki utjecaj na točnost prilikom verifikacije osoba. Bulatov, Jambawalikar, Kumar i Sethia definirali su 30 mjera koje se promatraju prilikom analize dlana (duljine, širine, polumjeri donjeg i gornjeg dijela, opsezi i površine prstiju, te površina dlana bez prstiju). [5]

Šarenica oka (*slika 7*) formira se od III do VIII mjeseca nakon začeća (pigment do 1. godine života), ne mijenja se tijekom života (osim u slučaju ozljede) i ne podliježe starenju, svaka je različita, kirurški ju je nemoguće krivotvoriti. Sukladno navedenom, prepoznavanje osobe pomoću šarenice jedna je od najsigurnijih biometrijskih metoda, a može se koristiti i u prisutnosti naočala i kontaktnih leća.[22]

Slika 7. Tehnika prepoznavanja šarenice oka [55]



Slika 8. Mrežnica [56]

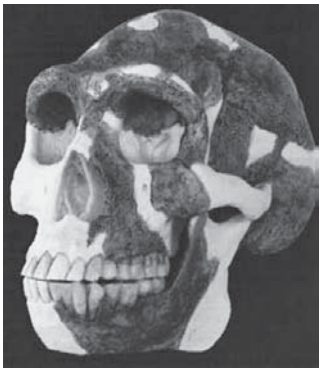


Ova metoda nije 100% pouzdana. Grupa njemačkih istraživača uspjela je prevariti jednu od komercijalnih verzija uređaja za prepoznavanje tako što su visokokvalitetnu sliku oka ispisali pomoću pisača visoke rezolucije, te u sredini probušili rupu. Tako je uređaj za dobivanje slike šarenice vidio „živu" zjenicu. [12]

Mrežnica (*slika 8*) je tkivo živčanih stanica koje se nalazi u stražnjem dijelu oka. Jedinstvena je svaku osobu zbog mreže krvnih kapilara kojima je prožeta, ne mijenja se tokom života osim u slučajevima glaukoma i dijabetesa. Slika mrežnice dobiva na način da se laserska infracrvena svjetlost usmjeri u unutrašnjost oka. Reflektirana svjetlost sadrži podatke o položaju kapilara.

Ova biometrijska metoda osigurava najveću točnost prepoznavanja. Ovo je ujedno i najskuplji način identifikacije jer je oprema kojom se vrši skeniranje mrežnice jako skupa. Skeniranje mrežnice traje 10-15 sekundi. Negativnost ove metode je njena odbojnost jer zahtijeva prodiranje laserske svjetlosti u oko osobe. Ima veliku primjenu u vojnim objektima, te područjima visokog stupnja sigurnosti (policijske postaje, zatvori, nuklearne elektrane, osjetljivi laboratoriji). [26]

Slika 9. Ostaci lubanje [57]



Prema *slici 9*, iz koje su vidljivi ostaci zubala, kada je riječ o identifikacijskoj odontologiji riječ je o dva aspekta, traseološkom i identifikacijskom. Prvi se odnosi na identifikaciju osoba

temeljem tragova zuba (ugriza, odgriza i sl) pronađenih na mjestu događaja, a drugi se odnosi na identifikaciju osoba i mrtvih tijela. Usporedba statusa zubala pronađenog mrtvog tijela nepoznate osobe vrši se sa statusom zubala iz zubnih kartona, rendgenskih snimaka zubala, medicinske dokumentacije o preboljenim traumama ili bolestima i sl. Osim utvrđivanja identiteta mrtve osobe može se raditi i o identifikaciji počinitelja i/ili žrtve koji je ostavio tragove zubi na drugoj osobi ili predmetima. [14] U postupku klasične identifikacije gleda se broj zubi, njihov položaj i raspored, veličina, razmak a zatim i osobitost zubi i zubala. Mogu se koristiti i tragovi stomatoloških zahvata poput popravaka, plombi, kruna, mostova i proteza. [22] Ova metoda ima ograničenu uporabu ako ne postoje centralizirane i ažurirane baze podatka što je slučaj u RH.

Oblik uha i struktura hrskavog tkiva na površini uha različiti su među osobama, ali za njih ne možemo reći da su jedinstvena osobina. Ta metoda je još u razvoju, te su potrebna dodatna istraživanja da bi se utvrdila pouzdanost metode mjerenja vektora duljina izbočenih točaka na površini od lokacije graničnih znakova uha. Nedostatak je što je u slučaju prekrivenosti uha kosom, tehnika neprimjenjiva. [22]

Mirisi koje emitira ljudsko (ili životinjsko) tijelo, različiti su za svaku jedinku. Biometrijski sustavi, bazirani na ovoj metodi, vrše analizu preko kemijskih senzora, od kojih je svaki osjetljiv na određenu grupu aromatskih smjesa. Sustav je vrlo skup i „elektronički nos" razvijan je za traženje droge i eksploziva, odnosno, kao osjetljivija zamjena za pse. Ipak, sustav je našao i primjenu u biometrijske svrhe kod nekoliko privatnih kompanija u Japanu i u Britanskoj ambasadi u Buenos Airesu. [48] Nedostatak je utjecaj kemijskih tvari na kvalitetnu detekciju mirisa (sapuni, parfemi, losioni, i sl.)

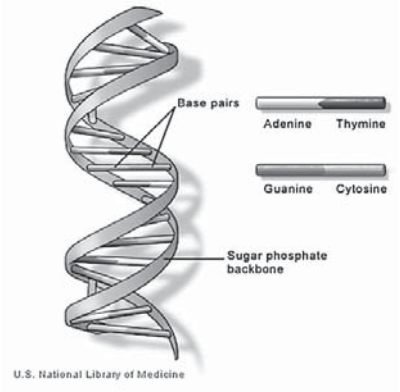
Analiza DNK (*slika 10*) jedna od najznačajnijih i najpouzdanijih biometrijskih metoda identifikacije. 99,5% DNK molekule je zajedničko svim ljudima i to područje DNK naziva se nekodirajuće područje, dok preostalih 0,5% predstavlja kodirajuća područja koja su visoko varijabilna (polimorfna), te čine svaku osobu jedinstvenom.

Analiza DNK koristi se u mnogim područjima istraživanja, a najzanimljivija primjena je u području kriminalistike i sudske medicine gdje se analiza DNK koristi za utvrđivanje identiteta nepoznate osobe, dokazivanje roditeljstva, posmrtnu identifikaciju ostataka mrtvog tijela, određivanje spola osoba, odnosno za traseološku identifikaciju (identifikacija osoba koji su u svezi s kaznenim djelom analiziranjem tragova biološkog podrijetla pronađenih na mjestu događaja), te kriminalistička istraživanja kaznenih djela, ali i za dokazivanje neopravdano osuđenih zatvorenika. [15] Nedostaci DNA metode se ogleda u tome što je to dugotrajan i skup proces analize koji uključuje stručno osposobljene osobe, DNA uzorci su osjetljivi, lako se onečiste. [13]

3.1.2. Ponašajne biometrijske karakteristike

Svaka osoba ima jedinstven rukopis, za potpis se može reći da je on kao neka vrsta otiska prsta osobe, koji se može iskoristiti u identifikaciji osobe. Ova metoda nije sigurna jer potpis se razvija i mijenja tijekom vremena, pod stalnim je utjecajem fizičkog i emocionalnog stanja. Postoje dva pristupa identifikacije potpisa: statički – promatra se geometrija potpisa i dinamički – promatra se geometrija potpisa, te brzina i putanja.

Slika 10. DNK analiza [58]



Glas nije jedinstvena karakteristika. Cilj autentifikacije glasom jest utvrditi tko je govornik uspoređujući pohranjeni uzorak s trenutnim. Oslanja se na karakteristike glasa, a ne na izgovor pojedinih riječi. Karakteristika glasa ovisi o građi glasnica, grla i usne šupljine, ali i o naučenim karakteristikama (tempu i stilu govora). Kako bi se mogla obaviti usporedba potrebno je pri registraciji od korisnika zatražiti da izgovori neku frazu.

Takav sustav je podložan prijevarama u kojima se glas legitimnog korisnika snimi i kasnije reproducira pri autentifikaciji. Sustav je osjetljiv na buku a glas varira o raspoloženju korisnika o njegovoj dobi, bolest, sl. Nedostatak je podložnost promjenama osobe kao što su (bolest, mutacija, problemi sa zubima i sl.), lako je imitirati. Predstavlja metodu koja se najviše koristi za identifikaciju putem telefona. [13]

Slika 11. Dinamika tipkanja [59]

Tehnika koja se razvila za vrijeme II svjetskog rata, kad je utvrđena razlika u dinamici tipkanja (*slika 11*) kod radiotelegrafista. Predstavlja nenametljivu tehniku koja se temelji na duljini držanja pojedine tipke, razmaku između dvaju pritisaka tipki kao i ukupnog vremena. [22]

Slika 12. RFID – radio frekvencijska identifikacija [60]

Granično biometrijsku tehnologiju, najmanje privlačnu, predstavljaju RFID implantati (eng. *RFID Chip Implants*) i koriste se u ekstremnim situacijama kao potpora ostalim metodama biometrije. Radi se o čipu ugrađenom ispod kože, koji sadrži unikatan identifikacijski broj zajedno s ostalim podacima i privilegijama nositelja čipa. Čip je pasivan i energiju dobiva bežično od samog čitača u trenutku očitanja, te s tom energijom šalje podatke u svojoj memoriji nazad čitaču. To su tehnologije koje su već našle svakodnevnu primjenu usprkos nekim svojim nedostacima. [44]

Slanost tkiva je novija tehnologija koja koristi elektroniku i ljudsko tkivo. Slanost tkiva (eng. *Body Salinity*) je nadogradnja tehnologije u nastajanju koju razvija IBM, a to je prijenos podataka preko kože. Na osnovi frekvencijskih odziva elektrolita u tkivu sustav autentificira korisnika, nakon čega se dodatni podaci mogu poslati kroz kožu s neke elektronike koja dodiruje kožu bilo gdje drugdje na tijelu. Ugrađivanje elektronike u tijelo ovdje nije potrebno. [44]

Slika 13. Metoda prepoznavanja krvnih žila [61]

Prepoznavanje žila (*slika 13*) na gornjoj strani ruke (eng.*Vein Pattern Recognition*) jedna je od takvih metoda kod koje se snimaju veće žile na stražnjoj strani ruke. Koristi se infracrveno osvjetljenje kojim se lako uočavaju žile pod kožom i zato se koristi za prepoznavanje žila na bilo kojem dijelu tijela. Prednost ovakve metode leži u činjenici da pozicije žila ostaju nepromijenjene kroz život i ne mogu se izbrisati ili jednostavno falsificirati. [25]

Pulsiranje krvotoka (eng. *Blood Pulse*) je srodna metoda, ali ona koristi i slike iz vidljivog područja, te uspoređuje uzorak u vidljivom i infracrvenom dijelu spektra koji stvaraju elementi kože. Uspoređuju se dubina na kojoj se nalaze kapilare i njihova brojnost, površinski pigmenti, pulsiranje krvnih žila i nakupine proteina u tkivu. [6]

4. Percipiranje biometrije od strane šire javnosti i primjena biometrijskih metoda u praksi

Na 15. kongresu o informacijskoj tehnologiji, održanom u svibnju 2006 godine, industrijske vođe su pozvane na proširenje definicije „sigurnosti" kako bi se obuhvatili novi trendovi globalizacije i novog sudaranja ekonomskih, političkih, potrošačkih sila te zahtijevaju više odgovornosti od poduzeća i vlada. Otvara se niz pitanja kako uspostaviti ravnotežu na jednu stranu novonastalih trendova otvorenog globalnog tržišta, brisanja granica a na drugu zaštita nacionalne sigurnosti, zaštita od kriminala, terorizma, ilegalnih migracija itd.

Kako osigurati pozitivnu identifikaciju ljudi i roba, a da se pri tom u potpunosti garantira sigurnost njihovih podatka, poštivanja ljudskih prava i sloboda, prava na privatnost te uzeti u obzir različitost kulturološku, etnički, vjersku, različitost zakonske regulative i razvijenosti pojedinih zemalja. Identitet i identifikacija značajan je čimbenik pri postizanju sigurnosti.[2] Kako u realnom svijetu postići ravnotežu između osobne privatnosti i sigurnosti s obzirom na nacionalne višenamjenske identifikacijske sustave.

Fokusirajući se na elektronički identitet, ulogu e-uprave i važnost očuvanja privatnosti, posve je jasno da pred vladama zemalja stoji velika odgovornost i zadatak u osiguranju sigurnosti. Tu se biometrija javlja kao sigurnija i pouzdanija metoda od svih tradicionalnih metoda identifikacije. No unatoč dostignućima biometrije, treba naglasiti da je ona samo jedan od alata za identifikaciju i uzeti u obzir da i biometrijski identifikacijski sustavi podliježu pogreškama i da nisu savršeni.

Posve je nevažno hoće li se elektronička identifikacija vršiti putem biomterijskih metoda kao što su skeniranje šarenice oka, otiskom prsta ili će se koristiti pametne kartice i sl. Važno je naglasiti da u pozadini stoji robusna tehnička infrastruktura kojom se vrši analiza podataka, pohranjivanje u bazu podatka, uspoređivanje, daljnja distribucija i da to zahtijeva postavljanje posebnih sigurnosnih protokola. Informatička infrastruktura postaje važna i od vitalnog nacionalnog značaja, poput infrastruktura željeznice, energetskog sustava i sl.

Voditeljica Odjela za povjerenje i sigurnost Europske komisije gospođa Sentucci, navodi: *„Identitet je jedno od najtežih pitanja koje treba riješiti zajedničkim snagama, zahtijevati će se zajedničko istraživanje i novi zakonodavni okvir"*. Nadalje, navodi da je *„cyberspace prostor postao velik i neograničenih mogućnosti, složenija društvena mreža u kojoj ljudi igraju različite uloge, različitih identiteta i pseudonima, lozinki i korisničkih imena"*. [23]

Neovisno je li osoba u cyberspace u interjekciji s vladinim institucijama, on –line trgovinama, ili prijateljima postavljaju se slijedeća pitanja:

1. kako možete biti sigurni da je to baš ta osoba za koju se netko predstavlja?
2. kako osoba može biti sigurna će njeni privatni podaci biti korišteni u mjeri kojoj ona želi?
3. kako upravljati sigurnošću osobe koja uspostavlja više različitih odnosa i radnji putem interneta?
4. koliko je cyberspace sigurno i zaštićeno okruženje i omogućuje li ukoliko je to potrebno hitnu pomoć putem intervencije policije?
5. koje mjere i standardi su potrebni za pouzdanost, povjerenje i zaštitu privatnosti?

Ova pitanja su važna jer se sudaraju osobno percipiranje sloboda cyber – prostora i sigurnosne politike (neovisno radi li se o pojedincima ili pravnim osobama) s sigurnosnim politikama ostalih sudionika, što naglašava potrebu pregovora o zajedničkoj sigurnosnoj politici. Studija kojom se sastojalo utvrditi percipiranje javnosti pojma identiteta, provjere i metode provjere identiteta, razlike u poimanju privatnosti i dijeljenje osobnih podataka, upravljanje podacima, obuhvaćala je analizu podataka o preferencijama ljudi koji žive u četiri različite regije u svijetu (Latinska Amerika, Sjeverna Amerika, Europa i Azija – Pacifik). [9] Studijom se svako nastojalo dobiti mišljenje javnosti o metodama identifikacije i narušavaju li biometrijske metode njihova prava na privatnost.

Mnoge organizacije djeluju na globalnom tržištu i kako bi im se osiguralo djelovanje van nacionalnih granica javlja se potreba upravljanja identitetom. Važno je da organizacije i vlade prilikom izgradnje metoda identifikacije ne krše kulture, društvene i etičke senzibilitete nacije ili regija svijeta.

Ispitanici su uglavnom spremni podijeliti značajni dio osobnih podataka kako bi dokazali ili potvrdili svoj identitet. Međutim, sklonosti pojedinaca su različite u pojedinim zemljopisnim regijama. Pojedinci u Sjevernoj Americi, Europi i Aziji – Pacifiku spremniji su podijeliti osobne podatke s vladom nego organizacijama nasuprot ispitanika u Latinskoj Americi. Ispitanici svih regija su spremni podijeliti više osjetljivi osobnih podataka ako bi se stvorilo „jedinstveno – višenamjensko uvjerenje o identitetu" koje bi se moglo koristiti u različite svrhe ali samo uz potvrdu da bi se radilo o snažnijoj verifikaciji i sigurnosti podataka. Prema ispitanicima, najvažnije funkcije za višenamjensko uvjerenje o identitetu bi bilo: prilikom prijevoza (zrakoplovi, vlakovi, autobusi), prelazak granice, pristup javnim mjestima (stadionima, zračnim lukama) i pristup Internet računu. Jako mali broj ispitanika korištenje višenamjenskog identiteta bi koristilo priliko ulaska u domove, na radno mjesto, kao zamjena za ključ automobila, mobitela.

Podatci koje su ispitanici spremni podjeli su ime i prezime, adresa, telefonski broj, dok su najmanje spremni podijeliti podatke koji uključuju rasu, religiju i broj kreditne kartice. Većina ispitanika bi voljela da se uvjerenje o identitetu nalazi na osobnoj iskaznici, a prijedlog o pohrani biometrijskih podataka na čipu implantat unutar njihov tijela, prihvatljiv je svega 10% ispitanika. Po pitanju sigurnosti osobnih podataka, u prosjeku, ispitanici svih regija vjeruju da bankarske institucije imale najvišu razinu zaštite i provjere osobnih podataka, dok većina ima najmanje pouzdanje i vjeru u policiju i ostale pravosudne organe.

Većina ispitanika svih regija pozitivno prihvaća uporabu biometrijskih metoda u svrhu provjere identiteta, dok su najpoželjnije metode za prepoznavanje glasa i otiska prsta, a najmanje poželjna metoda je skeniranje lica, skeniranje šarenice ili oka. Glavni razlog prihvaćanja biometrijskih metoda od strane ispitanika je po njihovom mišljenju, praktičnost (ne moraju pamtiti zaporke), učinkovitost (brzina provjere) i dokaza identiteta. Navedeni razlozi neprihvaćanje biometrijskih metoda u sustavu identifikacije, prije svega su sumnja kako ove tehnologije rade a onda strah od gubitka privatnosti, gubitka identiteta.

Elektronske identifikacije i upravljanje identitetima su posve novi koncept za većinu ljudi, koji zbog nedovoljne educiranosti, razumijevanja, osjećaju strah i nesigurnost. Značajni problemi koji se također javljaju su nejednaki stavovi među državama, nejednaka razvijenost i neujednačenost zakonske regulative, prakse i tehnologije. No, pitanja o identitetu i identifikaciji kao i pitanja upravljanja identitetima, sigurnosti svakim danom biti će sve više.

Nakon 11. rujna 2001 godine, ne samo u Americi nego diljem svijeta, pojačava se osjećaj nesigurnosti, ranjivosti i pojačanog straha od terorizma. Terorizam i međunarodni kriminal su također poprimili globalne razmjere te postaju ozbiljna prijetnja međunarodnoj zajednici. Amerika je od tad pojačala razinu sigurnosne kontrole, pokretač je usvajanja biometrijskih metoda i drugih tehnika prilikom granične kontrole. Kako se i Europa suočava sa sličnim problemima treba se zauzeti zajednički, koherentan pristup uvažavajući pri tom sve prije navedene potrebe i senzibilitet različitih zemalja, utirući tako put doista integriranoj i sigurnoj regiji i svijetu. Uvođenje i širu primjenu biometrije u svakodnevnom životu u Europi uzrokovala je odluka EU-a za provedbu biometrijskih značajki (lica i otiska prsta) u putovnici EU-a. Samo snimanje otiska prsta postaje nužan korak za sve više procesa a, korištenje ove metode je sve zastupljenije i u civilnoj primjeni

4.1. Primjena biometrijskih metoda

Biometrijski sustav nudi nekoliko prednosti u odnosu na tradicionalne sheme identifikacije i autentifikacije. Oni su sami po sebi pouzdaniji od lozinkom utemeljene autentifikacije, biometrijske značajke ne mogu biti izgubljene ili zaboravljene (lozinka se može izgubiti ili zaboraviti), teško ih je kopirati, dijeliti i distribuirati (dok lozinka može biti objavljena na hakerskim web stranicama), zahtijevaju od osobe da bude prisutna u vrijeme provjere dok to nije slučaj sa lozinkama (posjednik lozinke uopće ne mora biti vlasnik iste). Svaka biometrijska metoda ima svoje prednosti i nedostatke, a sam izbor ovisi o primjeni. Niti jedna biometrijska metoda ne udovoljava u potpunosti svim zahtjevima (npr. da je u potpunosti točna, praktična i da ne iziskuje velika financijska ulaganja). [12]

Primjena biometrijskih sustava može se podjeli u tri skupine:

1. komercijalne aplikacije kao što su pristup računalnim mrežama, elektronska sigurnost podataka, e-trgovina, pristup bankomatima, kreditne kartice, kontrola fizičkog pristupa, uredsko poslovanje, učenje na daljinu, području sigurnosti, zaštite i nadzora informacijskih sustava itd.;
2. aplikacije državnih institucija kao što su nacionalne osobne iskaznice, putovnice, vozačke dozvole, socijalno i zdravstveno osiguranje, pristup službama s visokom razinom sigurnosti;

3. medicinsko - forenzičke aplikacije poput onih za utvrđivanje identiteta nepoznate osobe, posmrtna identifikacija ostataka mrtvog tijela, u svrhu traseološke identifikacije i kriminalističkog istraživanja kaznenih dijela, utvrđivanje očinstva, dokazivanje roditeljstva , aplikacija za identifikaciju terorista u svrhu kaznenog progona itd. Za traseološku analizu primjena analize DNA od velike je važnosti za identifikaciju osoba koje su u svezi počinjenja kaznenog dijela, analiziranjem tragova biološkog podrijetla pronađenih na mjestu događaja (krv, sprema, dlake, slina, urin, tkiva, stanice i ostale tjelesne izlučevine).[20] Nadalje, koristi se odontologija kod utvrđivanja identiteta temeljem statusa zubala (utvrđivanje počinitelja kaznenog djela ili slučajevi utvrđivanja identiteta mrtve osobe). Poznata primjena biometrijske analize je daktiloskopija (analiza otiska prstiju i dlanova te analiza papilarnih linija u slučaju identifikacije počinitelja kaznenog djela ili slučajevi utvrđivanja identiteta mrtve osobe). AFIS sustav je moderni računalni sustav za automatiziranu obradu otisaka papilarnih linija prstiju i dlanova, a u svojoj bazi podataka sadrži pohranjene otiske.[19]

Biometrijske metode u sustavu sigurnosti, zaštite i nadzora informacijskih sustava zajedničke su za sve tri skupine primjene (komercijalne aplikacije, aplikacije državnih institucija i medicinsko – forenzičke aplikacije). U ovom području biometrijske metode koriste se za: zaštitu osobnih računala, telefona i interneta; ograničavanje neovlaštenog pristupa radnim mjestima i skladištima; autentifikacija pristupa prilikom e-bankarskih transakcija; sprječavanje krađa i krivotvorenja pri financijskim transakcijama; osiguranje graničnih prijelaza; osiguranje aerodromskih terminala; biometrija je svoju primjenu pronašla u osiguranju banaka; te osiguranje pristupa područjima visokog stupnja sigurnosti (policijske postaje, vojne institucije, zatvori, nuklearne elektrane, osjetljivi laboratoriji), nadalje u izradi putnih isprava kao što su putovnice i pomorske isprave. Primjenu biometrije nalazimo čak i među društvenim mrežama kao što je Facebook, Google, Yahoo itd.

Primjeri biometrijskih primjena:

a) sustav provjere otisaka prstiju proizveden od tvrtke Digital Persona, Inc, koristi se za računalne mreže i prijavu

b) otisak prstiju koristi se na prodajnim mjestima (POS) terminalima, proizveden od tvrtke Indivos, Inc, koji provjerava kupce i ubrzava plaćanje u maloprodajnim trgovinama, restoranima i menzama

c) brava otisaka prstiju koristi se na ulaznim vratima proizvedena od strane BioThentica Corporation koristiti za ograničavanje pristupa prostorijama

d)imigraciju i naturalizaciju ubrzava usluga sustava (INSPASS), koji je instaliran na glavnim zračnim lukama u SAD-u, temelji se na metodi provjere geometrije ruke, sustav je razvila tvrka Recognition Systems, Inc. i značajno smanjuje vrijeme obrade imigracije [13]

e) granični prolazni sustav koristi metode provjere i prepoznavanja šarenice u Londonskoj zračnoj luci Heathrow [43]

f) Zračna luka Ben Gurion u Tel Avivu (Izrael) koristi Express kartice za ulazak u kioske opremljene metodom provjere geometrije ruke [13]

g) Kanadska CATSA (eng. *Canadian Air Transport Security Authority*) koristi programe identifikacijskih kartica za kretanje ograničenim područjima zračnih luka. RAIC (eng. *Re-*

stricted Area Identification Card) a služi se biometrijskim podacima otisaka prstiju i skeniranjem šarenice za verifikaciju identiteta pojedinaca koji imaju dozvoljen pristup ograničenim područjima [47]

h) Zračna luka u Sydneyu je prva u svijetu uvela sustave SmartGate, kiosci koji imaju mogućnost skeniranja fotografije sa putovnice i elektroničkog uspoređivanja s licem osobe koja drži putovnicu [39]

i) Berlinska zračna luka prva u Europi uvodi sustave za prepoznavanje lica pod nazivom Zn-Face. Sustavi se koriste za osiguranje osjetljivih područja zračne luke, pohranjivanjem podataka registriranog osoblja na smart karticu s već poznatim postupkom identifikacije i kontrole pristupa [46]

j) FacePass sustav iz Viisage se koristi u POS verifikacijskim aplikacijama poput bankomata što uklanja potrebu za PIN-om [13]

k) (eng. *Identix Touch Clock*) sustav analize otiska prsta koristi u aplikacijama za provjeru radnog vremena djelatnika [13]

l) Danas banke širom svijeta biometriju koriste kao nešto uobičajeno, a primjena joj je vrlo široka. U Japanu je većina bankomata opremljeno sustavima za prepoznavanje otiska vena ili prsta. U Čileu i Brazilu danas su svi osobni dokumenti biometrijski, dok je prvi biometrijski bankomat u Europi instaliran sredinom 2011. u Poljskoj (BPA SA Bank) [40]

m) Biometrijska putovnica je javna isprava u svojoj strukturi sadrži elektronički „nosač" podataka – čip, koji je skriven unutar putovnice. Unutar čipa putovnice pohranjuju se: osobni podaci nositelja putovnice (ime, prezime, državljanstvo, datum rođenja, podatak o spolu, oznaka za vrstu putne isprave, oznaka države, broj putovnice, osobni identifikacijski broj, datum izdavanja i datum isteka valjanosti putovnice i tijelo koje je putovnicu izdalo) i biometrijski podaci nositelja putovnice (digitalizirana slika lica i otisci dva kažiprsta). Biometrijsku putovnicu RH-a je uvela poradi usklađivanja s međunarodnim standardima sigurnosti putnih dokumenata, kao elementa sigurnosti granica i putovanja. Biometrijska putovnica ima značajne prednosti nad dosadašnjom hrvatskom putovnicom: pruža još veću zaštitu od prijevarne zlouporabe i neovlaštenih izmjena; smanjuje rizik od „krađe identiteta"; pospješuje zaštitu hrvatske granice putem brze provjere nositelja hrvatskih putovnica koji ulaze u zemlju [45]

n) Društvene mreže kao što je npr. Facebook na ležeran način kroz zabavu i druženje, uz suglasnost samih korisnika, koristi također biometrijske metode i na taj način stvara bazu podataka „dosje" o svakom korisniku. Aplikacija za prepoznavanje lica može u gomili fotografija prijatelja pronaći osobu koju tražite, bez obzira na kut snimanja slike. Možete doznati podatke koliko ste često na mreži, tko su vam najdraži i prijatelji i oni s kojima najčešće komunicirate, tko vas prati, niz na oko bezazlenih podataka;

o) Google, između ostalog, koristi biometriju za analizu učinkovitosti oglašavanja na web stranici mjereći kod ispitanika kretanje očiju, pokrete miša, možđane funkcije i ostale mjerljive znakove pažnje i čitanja. Dobivena statistika im služi za mjerenje efektivnosti marketinške kampanje prije nego je uopće i započela. Google nije bio prvi. Yahoo! se također služi marketinškim biometrijskim metodama

Sigurnost cijelog sustava je dobra koliko najslabija njegova karika - zaporka. Konačno, kada se zaporka dijeli sa kolegom, ne postoji način da sustav zna tko je stvarni korisnik. Isto tako, postoje mnogi problemi sa ključevima, karticama za identifikaciju. Na primjer, ključevi i kartice mogu se dijeliti, umnožavati, izgubiti ili biti ukradeni a, i napadač može napraviti „master" ključ koji može otvoriti mnoga brave. Znatno je teže za kopiranje, dijeljenje i distribuciju biometrijskih značajki.

Biometrijska značajka ne može biti izgubljene ili zaboravljene, osoba u trenutku identifikacije mora biti osobno prisutna. Teško je krivotvoriti biometrijske značajke. Nadalje, svi korisnici sustava imaju relativno jednak stupanj sigurnosti i jedan račun nije lakše probiti nego bilo koji drugi. Biometrija uvodi nevjerojatnu pogodnost za korisnike (korisnik više ne mora pamtiti višestruke, dugačke i kompleksne zaporke niti ih mijenjati) zadržavajući dovoljno visok stupanj sigurnosti.

Za napad na biometrijske sustave, treba generirati (ili steći) velik broj biometrijskih uzoraka (npr. otisaka prstiju), što je puno teže nego što je generirati veliki broj pinova/zaporki. Sustav može kombinirati više različitih bimoetrijskih metoda npr.kombinirati lice i otisak prsta osobe ili otiske više prstiju čime se dodatno povećava sigurnost pristupa sustavu.

5. Analiza primjene biometrijskih metoda naspram tradicionalnih metoda sigurnosti, zaštite i nadzora informacijskih sustava

Tradicionalni dostupne tehnologije su metode temeljene na znanju (npr, PIN-ove i zaporke) i token-based metode (npr. ključeve i kartice). Većina korisnika postavlja svoje zaporke na temelju riječi ili brojki kojih se lako mogu sjetiti, kao što su imena i rođendani članova obitelji, omiljeni film ili glazbene zvijezde (provedena anketi je pokazala da od 1200 britanskih uredskih djelatnika, gotovo polovica je odabrala svoje ime, ime kućnog ljubimca, ili jednog člana obitelji kao zaporku, drugi temelje svoje zaporke na imenima kao što su Darth Vader i Homer Simpson). Takve zaporke lako je „probiti" po nagađanju ili pomoću jednostavnog brute force napada. [13]

Iako je moguće, pa čak i poželjno, da korisnici posjeduju različite zaporke za različite aplikacije i mijenjaju ih što češće, većina ljudi koristi istu zaporke za različite aplikacije i rijetko ili gotovo nikada ih ne mijenja. Ako je ugrožena jedna zaporka, to može dovesti do povrede sigurnosti ostalih aplikacija. Na primjer, haker može stvoriti lažnu internetsku stranicu koja korisnicima omogućava slobodnu registraciju na web putem korisničkog imena i zaporke. Haker može onda pokušati koristiti isto ime i zaporke za napad korporativnih računa korisnika, a najvjerojatnije i uspjeti u tome. Dulje zaporke su sigurniji, ali teže ih je pamtiti, neki korisnici ih zapisuju na dostupnim mjestima (npr. na "post-it" note) i sakriju ga ispod tipkovnice. Jake lozinke teško je zapamtiti i rezultiraju većim brojem Help Desk poziva. Nadalje, haker treba razbiti samo jednu zaporku među svim zaposlenicima kako bi dobio pristup Intranetu tvrtke i tako, jedna slaba zaporka ugrožava cjelokupni sustav tvrtke. [13]

Korištenje biometrijskih metoda pokazalo se sigurnije i pouzdanije od korištenja bilo koje tradicionalne metode identifikacije ali svakako treba uzeti u obzir da i navedeni sustavi imaju svoje nedostatke, ograničenja i slabosti. Kao što je ranije spomenuto, razina točnost sustava identifikacije i provjere putem otiska prsta, usporena je i otežana ukoliko sustav radi usporedno veliki broj analiza (npr. u američkoj zračnoj luci prosječno u danu prođe 200 000 tisuća

putnika, sustav će imati 99% šanse za hvatanje kriminalaca ali također će zbog preopterećenja, sustav imati minimalno 200 lažnih uzbuna). [12] Nadalje, ako se koristilo lice kao metoda identifikacije umjesto otisaka prstiju, broj lažnih uzbuna će biti znatno veći, s obzirom na prilično nisku točnost sustava identifikacije lica, osobito u sredinama gdje vlada velika gužva, gdje su različiti svjetlosni uvjeti, osoba može prekriti lice da se ne vidi itd.

Biometrijski sustavi ne mogu još uvijek u potpunosti samostalno precizno podržavati identifikacijske provjere. U takvim poluautomatskim aplikacija, biometrijski sustav samo generira alarm koji poziva na bliže (ručno) ispitivanja pojedinca i alarm na izravno provjeru radi li se zaista o mogućoj kriminalnoj osobi ili teroristi. Uspješne instalacije biometrijskih sustava u različitim područjima djelovanja ne znači da će biometrija u potpunosti riješiti sve sigurnosne problem. Jasno je da postoji dosta prostora za poboljšanje biometrijskih metoda, istraživači ne rješavaju samo probleme vezane uz smanjenje stope pogrešaka, oni također traže načine kako bi se poboljšala iskoristivost biometrijskih sustava.

Biometrijski sustavi koji u radu koriste bilo koji pojedinačnu biometrijsku značajku imaju sljedeća ograničenja: [13]

1. kod provjere glasa - buka u pozadini, iskrivljenost glasa od hladnoće ili bolesti ili straha,
2. kod provjere otiska prsta, prsti mogu biti sa ožiljkom ili posjekotinom, masni, vlažni ili npr.senzor za očitavanje nije čist,
3. kod provjere lica, postoji mogućnost nepovoljnih uvjeta okoline, gužva, loša rasvjeta, prikrivenost lica, loš kut snimanja lica, sličnosti geometrije lica,

Ranjivosti biometrijskog sustava su: napadač može prijevarom dobiti pravo pristupa sustavu, analizirati osjetljive podatke kao što su medicinske evidencije, mijenjati podatke, brisati, uključujući i biometrijske značajke; ovlašteni korisnici mogu vršiti zlouporabu pristupa i tvrditi da je napad izvršen iz vani npr. bankovni službenici mogu mijenjati financijske podatke o kupcu; administratori baza mogu namjerno mijenjati biometrijske parametre sustava kako bi omogućili zlonamjerne upade iz vani; napadač može prisiliti legitimnog korisnika (npr.uz prijetnju vatrenim oružjem) da mu odobri pristup sustavu; napadač može preplaviti resurse sustava do točke gdje legitimnom korisniku pristup može biti onemogućen (npr. poslužitelj koji obrađuje zahtjeve pristupa može se bombardirati s velikim brojem lažnih zahtijeva, čime se opterećuju svi računalni resursi i sprječava obrada valjanih zahtijeva).

Biometrijski sustav kao i drugi sigurnosni sustavi je ranjivi na brojne neprijateljske napade, važno je riješiti pitanje sigurnog dizajna bimetrijskog sustava. Naime, jedan od sigurnih načina je kombiniranje bimetrijske autentifikacije i kriptografskih tehnika. Stvaranjem kombinirano biometrijski kriptografskog ključa koji je kritografski siguran (npr. neće uljezima otkriti informacije o biometrijskim značajkama ili o kriptografskom ključu) dok legitimnom korisniku omogućava pristup sustavu. U tradicionalnoj simetričnoj kriptografiji, ako šifriranje i dešifriranje nije putem identičnog ključa, operacija dešifriranja će proizvesti niz slučajnih i beskorisnih podataka. U slučaju biometrijskih identifikatora legitimni korisnik je „ključ“ u kontekstu kriptografskog sustava. [27]

Upravo poradi navedenih ograničenja i ranjivosti sustava naglašava se potreba korištenja multimodalnih biometrijskih sustava.[11] Neka od ograničenja nametnuta od strane unimodalnog biometrijskih sustava mogu se riješiti korištenjem više biometrijskih značajki (poput

lica i otiske prstiju osobe ili više prstiju osobe). Ovi sustavi su također u stanju zadovoljiti stroge zahtjeve izvedbe nametnute od strane raznih aplikacija [8]. Multimodalni biometrijski sustavi riješio problem nejedinstvenosti, budući da se korištenjem višestrukih značajki osigurali dovoljnu pokrivenost stanovništva. Nadalje, multimodalni biometrijski sustavi pružaju „eng. antispoofing" protuprovalne mjere, otežavajući uljezu istovremeno lažiranje više biometrijskih značajki legitimnog korisnika. Sustav osigurava da se „uživo" korisnik identificira i da je uistinu prisutan na mjestu i u trenutku identifikacije.

Multimodalni Biometrijski sustavi su dobili punu pozornost u novijim istraživanjima. Brunelli i sur. [4] opisuju multimodalni biometrijski sustava koji koristi osobine lica i glasa pojedinca za identifikaciju. Njihov sustav kombinira odgovarajuće rezultate pet različitih uvjeta koji djeluju na glasovne mogućnosti i lice da se dobije jedan sveukupni rezultat koji se koristi za identifikaciju. Bigun i sur. razvijaju statistički okvir na temelju Bayesian statistike za integraciju podataka prezentiranih po govoru (text-ovisna) i lice podaci korisnika.[1] Hong i sur. rade kombinacije lica i otisaka prstiju za identifikaciju osoba [10].

5.1. Etička strana biometrijskih metoda

Tanka linija je između nužnosti poradi opće sigurnosti i kršenja prava na privatnost i zajamčene slobode. Svjetski moćnici kreiraju trend neophodnosti nadziranja, identifikacija, strožih kontrola, opravdavaju ga činjenicom da je globalni terorizam u porastu a biometrijski sustavi bi djelovali preventivno u sustavu sigurnosti, nadzora i kontrole. Nalazimo li se pod teretom pretjerane sigurnosti, zadire li „veliki brat" u ljudsku slobodu i privatnost ili je takav nadzor zaista opravdan poradi sveopćeg dobra i sigurnosti ?

Također se postavlja pitanje identifikacije ljudi koji nisu u mogućnosti identificirati se (npr.djeca, starije osobe koje pate od demencije) ili drugih ranjivih skupina (osobe s invaliditetom, ovisnici o drogama, imigranti), postavljaju se etička pitanja jer se radi o populaciji koja nema ili je bitno umanjene sposobnosti odlučivanja i davanja pristanka na identifikaciju. Zaštita osobnih podataka unutar informacijskih sustava danas postaje jedno od najznačajnijih društvenih pitanja i ima iznimno značajnu ulogu. Nedopušteno otkrivanje podataka o osobnim značajkama poput spola, nacionalne pripadnosti ili pak nekog od biometrijskih podataka mogu negativno utjecati na pojedinca. [3] DNK biometrijske značajke mogu otkriti širok spektar medicinskih informacija o pojedincu uključujući i potencijalne bolesti, može nam otkriti što pojedinac pije, uzima li drogu, podatke o trudnoći, čime se povećava rizik od diskriminacije i zlouporabe podataka.

Uvijek će biti pojedinaca i grupacija koje neće prihvaćati biometrijske sustave kao opciju identifikacije, bilo iz vjerskih, ideoloških razloga, ili brige za zdravlje ali društvo neće dopustiti pojedincima da svojim ponašanjem kompromitiraju i dovedu u pitanje cijeli „sigurnosni" sustav. Biometrija i biometrijski sustavi već su danas toliko razvijeni da više ne postoji segment društva u kojem se ne pojavljuju.

6. Zaključak

Provedenom analizom raspoloživih podataka koji obrađuju navedenu problematiku, analizirana su tri usko povezana područja:

1. pojam informacijskog sustava, područje informacijske sigurnosti i što je određuje, sigurnosnih rizika i procjenu rizika, te upravljanje informacijskom sigurnošću:

neovisno o kojem se poslovnom sustavu radi (veličini sustava ili djelatnosti koju obavlja) gotovo je nezamislivo njegovo funkcioniranje bez podrške informacijskog sustava. Razina kompleksnosti informacijskog sustava, upravljanje sustavom informacijske sigurnosti, procjena rizika, efikasnost i funkcionalnost samog sustava u potpunoj je ovisnosti o odlukama i postavljenoj sigurnosnoj politici same organizacije u skladu s propisanim zakonima. Informacijski sustavi organizacija, bilo da se radi o državnim tijelima ili pravnim osobama svakodnevno su izloženi sigurnosnim napadima, a upravljanje sigurnosnim rizikom jedan je od temeljnih elemenata upravljanja sigurnošću informacijskog sustava i smanjenje rizika na prihvatljivu razinu.

Uvođenje informacijske sigurnosti ne podrazumijeva samo propisivanje sigurnosne dokumentacije sa sigurnosnim protokolima i procedurama, nego zahtijeva i strogo provođenje istih. Dobro postavljen sustav sigurnosti informacijskog sustava podrazumijeva kontinuirano planiranje i evaluaciju sigurnosne politike, proces praćenja rezultata analize sigurnosnih incidenata te prijavu slabosti sustava, procjenu rizika. Nužno je sustavno usklađivati, nadzirati, educirati osoblje i koordinirano provoditi propisane mjere i standarde sukladno zakonu i propisanoj sigurnosnoj politici. U suprotnom, propisani dokumenti sigurnosne politike gube smisao i ostaju samo hrpa propisanih protokola i procedura a informacijski sustav ostaje posve nezaštićen.

2. Pravno uređenje informacijske sigurnosti, središnja tijela nadležna za informacijsku sigurnost u RH, primjena pravila zašite podatka Europske unije i njenih članica, sustav normizacije informacijskih sustava te propisane norme za sigurnost informacijskih sustava:

smisao pravnog uređenja informacijske sigurnosti je postizanje adekvatnih sigurnosnih kriterija na razini države. Doneseni zakoni određuju pravni okvir informacijske sigurnosti. S važećim zakonima moraju se uskladiti svi propisani dokumenti sigurnosne politike ostalih subjekata. U RH jasno su postavljenja središnja tijela nadležna za pitanja informacijske sigurnosti. EU također postavlja zakonodavni okvir informacijske sigurnosti, zaštiti osobnih podatka a, sve članice unije imaju obvezu sa propisanim direktivama uskladiti nacionalne zakone. Direktive imaju za cilj ukloniti prepreke na protok osobnih podataka koji zahtijevaju visoku razinu zaštite temeljnih prava, posebno prava na privatnost u državama članicama. Poticanje integracije, brisanje granica, povećavaju se gospodarske aktivnosti, širi se tržište, povećava se mobilnost ljudi, roba, usluga i kapitala a to sobom donosi napredak i nove mogućnosti ali i rizike. No, tu se pojavljuju problemi i pitanja kako uslijed novonastalih trendova, otvorenog tržišta i brisanja granica u uniji na ujedinjenom području, uspostaviti ravnotežu i pomiriti razlike između nacionalnih i zajedničkih interesa.

U kontekstu informacijske sigurnosti i slobodnog protoka bimetrijskih podataka, postavlja se pitanje kako uspostaviti sigurnosni okvir na razini unije uvažavajući ljudska prava i slobode, prava na privatnost a pri tom pomiriti različitosti članica kulturološke, etničke, vjerske. Posebni problem koji se javlja je još uvijek neujednačenost zakonskih regulativa, praksa i tehnološka razvijenost članica. U zajedničkom interesu svih članica trebalo bi biti postavljanje jedinstvenog zakonskog okvira unutar unije, uvažavajući nacionalna zakonodavstva te

etička načela, prava i slobode svakog pojedinca. Posebno se naglašava potreba ujednačavanja standarda.

3. Pojam biometrije, povijest i razvoj biometrije, biometrijske metode, biometrijske sustave, percipiranje biometrije od strane šire javnosti, primjena biometriskih metoda, prednosti i nedostaci biometrijskih metoda nasuprot tradicionalnih metoda identifikacije, etička strana biometrijskih sustava:

korištenje biometrijskih metoda pokazalo se sigurnije i pouzdanije od korištenja bilo koje tradicionalne metode identifikacije. Bez pouzdanih sustava osiguranja osoba i imovine, ugrožene su brojne svakidašnje aktivnosti. Značajan čimbenik pri postizanju sigurnosti je identifikacija osobe. Provjera podataka mora biti brza, pouzdana, sigurna i da ne zadire u privatnost osobe. Do sada se provjera identiteta vršila isključivo pomoću sigurnosnih zaporki, kartica, pin kodova i vlastoručnih potpisa, no to u današnje vrijeme postaje sve nepouzdanje i ograničavajuće. Biometrija svakodnevno postaje sve češći oblik autentifikacije u različitim sferama života pa ja tako korištenje automatiziranog sustava radi prepoznavanja nečijeg identiteta, praćenjem njegovih fizičkih karakteristika ili ponašanja, već duže vrijeme dio stvarnosti.

U radu je prikazan različit način percipiranja pojedinaca pojma identifikacije, provjera i metoda provjere, i dalje je za većinu elektronska identifikacija posebno putem biometrijski značajki i upravljanje identitetima, još uvijek nov i nepoznat koncept te nemaju dovoljno povjerenja. Nedovoljna prihvatljivost, strah i sumnja pojedinaca u navedene metode uglavnom proizlazi iz nedovoljnog poznavanja metodologije prikupljanja biometrijskih uzoraka koje bi svoju primjenu imale u sustavu identifikacije, nadalje i sumnja kako ovi sustavi rade, gdje i tko će se podatke čuvati te strah od zlouporabe osobnih podataka, gubitka privatnosti i identiteta. I ovdje se kao značajan problem pojavljuje nejednakost stavova država, nejednakost i neujednačenost zakonske regulative, prakse i tehnologije.

Upravo je identitet i identifikacija značajni sigurnosni čimbenik preko kojeg vlade država, nadležna ministarstva, agencije u čijoj je nadležnosti osiguranje nacionalne sigurnosti, vide rješenje problema brisanja granica i svi promjena koji sobom nosi globalizacija. Biometrijski sustavi, neovisno kojom biometrijskom metodom se služe, pokazali su se kao sigurna, pouzdana, brza metoda identifikacije spram tradicionalnih metoda identifikacije (pomoću zaporki, pametnih kartica itd). Svaka biometrijska metoda ima svoje prednosti i nedostatke, a sam izbor ovisi o primjeni. No unatoč dostignućima biometrije, treba imati na umu da je ona samo jedan od alata koji se može koristi u sustavu identifikacije te da ne postoji savršena metoda koja ne podliježe pogreškama. Posebno je važno naglasiti da u pozadini stoji robusna tehnička infrastruktura kojom se vrši analiza, pohrana podataka u bazu, uspoređivanje, daljnja distribucija i da pristup takvim sustavima zahtijeva postavljanje posebni sigurnosnih protokola. Tu se opet otvaraju slijedeća pitanja u nadležnosti koje institucije će biti čuvanje pohranjenih biometrijskih podatka, pitanje sigurnosti distribucije podataka i tko sve će imati pravo korištenja podataka. Postojeća zakonska regulativa je dobar temelj za uređenje navedenih pitanja.

Biometrijski sustavi su u tolikoj mjeri razvijeni da su već pronašli svoju širu primjenu u društvu. Primjerice od osiguranja banaka, ustanova sa visokim stupnjem sigurnosti, graničnih prolaza, zračnih luka itd. U kontekstu korištenja biometrijskih metoda u sustavu sigurno-

sti, zaštite i nadzora informacijskih sustava biometrijske metode se također primjenjuju, u svim aspektima (komercijalnim aplikacijama, aplikacijama državnih institucija i medicinsko – forenzičkim aplikacijama) poslovanja. Koriste se za zaštitu osobnih računala, telefona, pristupa mrežama, neovlaštenog pristupa uredima, skladištima, sprječavanju krađa i krivotvorenja pri financijskim transakcijama itd. Šira primjena ovisi o razvijenosti države, same organizacije, postavljenoj sigurnosnoj politici organizacije, procjeni rizika organizacije i spremnosti na ulaganja u modele zaštite. Odabir modela sigurnosne zaštite ovisi također i o dostupnosti i cijeni sustava na tržištu.

Stoga, temeljem navedenog iznosimo slijedeće zaključke:

1. globalizacija mijenja svijet i donosi posve novu dimenziju u svim sferama društva, političkim, ekonomskim, sociološkim, financijskim i tehnološkim;
2. brz razvoj digitalne, informacijske i komunikacijske tehnologije, sveprisutnost Interneta snažno utječu na društvo, koliko god sobom nose napredak otvaraju se i nove dimenzije nesigurnosti koju sobom nosi povećana dostupnost podataka;
3. nedostatak zakonskog uređenja primjene biometrijskih tehnologija pri čemu ističemo prijedlog dopune postojećeg zakonskog okvira i pravne definicije biometrije kao elementa sigurnosti, zaštite i nadzora informacijskih sustava;
4. potreba za stvaranjem sigurnosnog okruženja postaje sve kompleksnija i zahtjevnija;
5. bez uvođenjem sustava informacijske sigurnosti nemoguće je osiguranje funkcioniranja poslovnih sustava i sustava upravljanja te svođenja rizika na prihvatljivu razinu;
6. organizacije (neovisno radi li se o državnim tijelima ili pravnim subjektima) trebaju sustavno vršiti usklađivanje, nadzor i koordinirano provoditi propisane standarde i mjere sukladno zakonu i propisanoj sigurnosnoj politici;
7. bez pouzdanih sustava osiguranja osoba i imovine, ugrožene su brojne svakodnevne aktivnosti. Značajan čimbenik pri postizanju sigurnosti je identifikacija osobe. Provjera podataka mora biti brza, pouzdana, sigurna i da ne zadire u privatnost osobe.
8. Korištenje biometrijskih metoda pokazalo se sigurnije i pouzdanije od korištenja tradicionalnih metoda identifikacije;
9. svaka biometrijska metoda ima svoje prednosti i nedostatke, a sam izbor ovisi o području primjene. Unatoč dostignućima biometrije, treba imati na umu da je ona samo jedan od alata koji se može koristi u sustavu identifikacije, da ne postoji savršena metoda koja ne podliježe pogreškama.
10. Biometrijski sustavi su pronašli svoju širu primjenu u društvu, od osiguranja banaka, ustanova sa visokim stupnjem sigurnosti, graničnih prolaza, zračnih luka itd.
11. Biometrijske metode identifikacije poboljšale su sigurnosna rješenja za kontrolu graničnih prolaza, pitanja migracije.
12. U sustavu sigurnosti, zaštite i nadzora informacijskih sustava biometrijski sustavi također imaju širu primjenu u svim aspektima poslovanja.
13. Šira primjena biometrijskih sustava ovisi o razvijenosti države, same organizacije, postavljenoj sigurnosnoj politici organizacije, procjeni rizika organizacije i spremnosti na

ulaganja u modele zaštite. Odabir modela sigurnosne zaštite ovisi također i o dostupnosti i cijeni sustava na tržištu.

14. U kontekstu informacijske sigurnosti i slobodnog protoka podatka na razini Europske unije javlja se potreba da članice zauzmu jedinstveni stav oko pitanja biomerijskih sustava, uvažavajući pri tom različitosti stavova, nacionalnih zakonodavstava, prakse i tehnologije.
15. Naglašava se potreba ujednačavanja standarda za kvalitetu prikupljenih biometrijskih značajki (npr.slika lica, slika otiska prsta itd.).
16. Potrebno je uvrstiti dodatne sigurnosne protokole i zahtjeve kako bi se poboljšala sigurnost i nemogućnost neovlaštenog pristupa, te mogućnost krivotvorenja i falsificiranja.

LITERATURA

[1] Bigun,S,E., Bigun,J., Duc,B. and Fischer, S., Expert concilation for multimodal person autentication system usnig bayesian statistics, in Proc.Int.Conf.Audio and Video-Based Biometric Person Authentication (AVBPA), Crans-Montana, Switzerland, Mar.1997,pp.291-300

[2] Bimetrics in Europe, Trend Report, European Biometrics Portal, Brussels, June 2006

[3] Boban, M., „Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu", Zbornik radova Pravnog fakulteta u Splitu, god. 49,3/2012. str. 575-598

[4] Brunelli, R. and Falavigna, D., Person identification using multiple cues., IEE Trans, Pattern Anal.Machine Intell., Vol 12,pp.955-966, Octob. 1995

[5] Bulatov Y, Jambawalikar S, Kumar P, Sethia S : Hand recognition using geomatric classifiers, *1st International Conference on Biometric Authentication (ICBA)*, Hong Kong, China, July 15-17, 2004. Editors: David Zhang and Anil K. Jain. LNCS 3072, pages 753-759. Springer

[6] CARNet (Croatian Academic and Research Network) : Biometrija, CCERT-PUBDOC-2006-09-167

[7] Čerić, V., Varga, M., Informacijska tehnologija u poslovanju, Sveučilište u Zagrebu, Element, Zagreb, 2004.

[8] Directive 95/46/EC of the European Parlament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Official journal of the European communities, No. L. 281., 1995.

[9] Global Study on the Public's Perceptions about Identity Management, Unisys funded research independently conducted by the Ponemon Institute LLC, 2006. – Published on the European Biometrics Portal.

[10] Hong.L, Jain,A.K., Integration faces and fingerprints for personal identification., IEEE Trans, Pattern Anal.Machine Intell., Vol 20, pp. 1295-1307, Dec.1998.

[11] Hong. L, Jain,A.K and Pankanti, S., Can multibiometrics improve perfomance?, in Proc. Autol ID' 99, Summit, NJ, Oct. 1999, pp 59-64.

[12] Jain,A.K, Ross,A., Pankanti,S.,Biometrics:A tool for Infromation Security, IEEE Transaction on Infromation Forensics and Security, Vol. 1, No.2., June 2006.

[13] Jain,A.K, Ross,A., Pankanti,S.,Biometrics:An Introduction to Biometric Recognation, IEEE Transaction on Infromation Forensics and Security, Vol. 14, No.1., January 2004.

[14] Jain,A.K, Ross,A., Pankanti,S., Prabhakar, S., Hong, L., Waymasn, J.L., Biometrics Tutorial, Michigan State University, 2005.

[15] Jurković K, i dr. Vrednovanje DNA analize u predmetima vještačenja prije DNA tehnologije. Policija i sigurnost br. 1 – 2 /04, st. 42.

[16] Kaluszynski M, Republican Identitiy: Bertillonage as government Technique, „Documenting Individual" edited by Jane Caplan & John Torpey.

[17] Kolarić – Gregorić T. Kriminalistička identifikacija osoba, Krimarak , Zagreb, MUP RH, 2002, 3-5.

[18] Klaić, A., Perešin, A., Koncept regulativnog okvira informacijske sigurnosti, Međunarodne studije, Zagreb, 2010.

[19] Pavišić B, Modly D, Veić P, Kriminalistika 1, Zagreb, Golden marketing – Tehnička knjiga.

[20] Peltier, T. R., Information Security Policies and Procedures, Auerbach Publications, 2004. PMI, A Guide to the Project Management Body of Knowledge, 3rd Ed., Project Management Institute, 2004.

[21] PMI, A Guide to the Project Management Body of Knowledge, 3rd Ed., Project Management Institute, 2004.

[22] Radmilović Ž, Stručni članak, Biometrijska identifikacija, 2008, str. 173.

[23] Santucci, G.:Presentation given at the seminar „Safe Mobility of People and Goods in a Greater Europe", Saint- Paul de Venece, 2004.

[24] Strenburner, G., Goguen, A., Feringa, A., Risk Management Guide for Infromation Tehnology System, NIS – National Institute of Standard and Tehnology, U.S. Department of Commerce, July 2002.

[25] Technology Assessment: Using biometrics for border security, GAO, 2002.

[26] Triantaphyllou, E., Multi – Criteria Decision Making Methods, A comparative Study, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2000.

[27] Valacich, J., and Schneider, C., Information Systems Today: Managing in the Digital World, Fourth Edition, Published by Prentice Hall.Copyright © 2010 by Pearson Eduction, Inc.

[28] Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima (NN br. 72/07),

[29] Uredba o mjerama informacijske sigurnosti (NN br. 46/08),

[30] Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima (NN br. 102/07)

[31] Zakon o informacijskoj sigurnosti, (NN br 79/2007)

[32] Zakon o zaštiti osobnih podataka (NN br. 103/03, 118/06, 41/08, 130/11, 106/12)

[33] Zakon o sigurnosno – obavještajnom sustavu RH (NN br. 79/06 i **105/06)**

[34] Zakon o tajnosti podataka (NN br. 79/07) ,

[35] Zakon o pravu na pristup informacijama (NN. 172/03.)

[36] Zakon o sigurnosnim provjerama (NN br. 85/08 i 86/12),

[37] Zakon o elektroničkoj ispravi (NN br.150/05),

[38] Wayman. J., Janin.A., Maltoni. D., Maio.D: Biometric Systems, Tehnology, Design and Performacne Evaluation, Springer, 2005.

Web izvori:

1. Australian Government:Australian Customs and Border Protection Service, dostupno na stranici: http://www.customs.gov.au/ Preuzeto: (30.07.2014.)
2. Emer M.Biometrija u bankama http://zastita.info/hr/clanak/2011/9/biometrija-u-bankama-sve-cesce-rjesenje,198,6133.html Preuzeto: (03.07.2014.)
3. EU zakonska regulativa dostupno: http://www.lexeurope.eu/en/domaine-intervention.html Preuzeto: (05.07.2014.)
4. HRN ISO/IEC 27001:2005, HRN ISO/IEC 17799:2005, Preuzeto sa www.hzn.hr, www.iso.org Preuzeto:(18.07.2014.)
5. MiSense Summary Report : Biometrically enabled access control trial at Heathrow Airport 2006/07, dostupno na stranici: http://www.libertysecurity.org/IMG/pdf/Trend_Report_2006.pdf Preuzeto: (30.07.2014.)
6. Mustač V, članak Tehnološki noviteti u biometriji, dostupno na stranici : http://www.gradimo.hr/clanak/tehnoloski-noviteti-u-biometriji/37599 Preuzeto: (07.07.2014.)
7. Izrada dokumenata – Putovnica, dostupno na stranici: www.mup.hr Preuzeto: . (30.07.2014.)
8. Smart Card News, 2002., Oct, 15th: Face Recognition At Berlin Airport dostupno na stranici: http://tcnwo.blogspot.com/p/national-id-cards.html Preuzeto: (30.07.2014.)
9. Simplifying Passenger Travel Interest Group: Heathrow Biometrics, dostupno na stranici:http://www.accenture.com/SiteCollectionDocuments/PDF/miSenseBiometricsTrialHeathrow.pdf Preuzeto: (26.07.2014.)
10. Tehnika i oprema: Nove metode sigurnosti putnika, Dostupno na stranici: www.zrakoplovstvo.net Preuzeto: (30.07.2014.)

Summary

BIOMETRICS IN SAFETY, PROTECTION AND SURVEILLANCE OF INFORMATION SYSTEMS

Encouraging integration into emerging global society, economic, and cultural connections with the rest of the world, the overall development is creating new opportunities and new risks. On one side are deleted borders and increased mobility of people, the flow of goods, capital, and economic activity. The rapid development of digital information and communication technology, the ubiquity of the Internet, has become a part of we usually often are not aware of their impact. The growing connectivity infrastructure, transport, energy, health and other areas with information technologies, increases the vulnerability of modern society. As much as technology has made the world safer and more advanced, it has opened the door to some new dimensions of crime. The complexity of creating a secure environment is extremely growing. Without a reliable system of security of persons

and property are threatened in many everyday activities. A significant factor in achieving security is to identify the person. Until now, the identity checks were made solely by means of secure passwords, card, pin codes and personal signatures, but that nowadays is becoming more restrictive and distrustful. Biometrics is an increasingly common form of authentication in different spheres of life.

Each biometric method has its advantages and disadvantages, and the choice depends on the application. But despite the achievements of biometrics, it should be remembered that it is only one of the tools that can be used in the identification system and that there is no perfect method that is not subject liable to errors. It is especially important to emphasize the complex technical infrastructure that is in the background, which are analyzed and data storage in a database, checking data, further distribution of data, and that access to such systems requires a special set of security protocols. Questions of keeping the biometric data stored, security and distribution of data and control that will be entitled to use the information are questions that need to provide a common response of the Heads of State Union. Existing legislation is a good basis for the regulation for these issues.

Keywords: *information systems, information security, security risk, risk prevention, legislation, biometrics, biometric systems.*