## 25.1 Organizacija sistema za zaštitu od provale

Svi neželjeni događaji koji su predmet otkrivanja u sistemu za zaštitu od provale neraskidivo su povezani za čoveka, počev od krađe, preko podmetanja požara do najrazličitijih oblika diverzije. Zbog toga je uloga tehničkih sredstava i uređaja u zaštiti od provale neophodna, imajući u vidu da bi samo fizičko obezbeđivanje zahtevalo angažovanje velikog broja ljudi, a u nekim slučajevima bi bilo i neizvodljivo. Sa druge strane, pošto je suština neželjenog događaja upad „uljeza“ u prostor ili objekat, postoje tri grupe mera koje mogu da se primene da se to spreči:

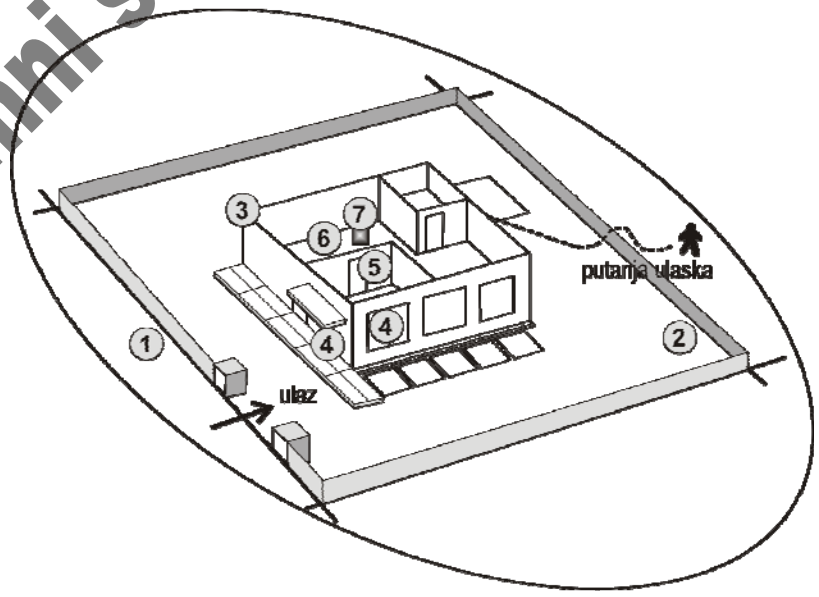
- mere kojima se sprečava ili otkriva neželjeni ulaz u prostor ili u objekat,
- mere kojima se posle ulaska lica otkriva kretanje u prostoru ili objektu i
- mere kojima se vrši legitimisanje ili identifikacija lica.

Iako navedene mere mogu da se realizuju pomoću fizičkih barijera, prepreka i angažovanjem obezbeđenja, pouzdana realizacija navedenih mera je gotovo nemoguća bez upotrebe tehničkih uređaja i sredstava - sistema za zaštitu od provale i sistema za kontrolu pristupa.

S obzirom na činjenicu da je nemoguće predvideti sa koje strane prostora ili objekta će doći do ulaska, kao i samo kretanje u prostoru koji se štiti, dobra organizacija zaštite od provale podrazumeva odbranu u koncentričnim krugovima, tako da savladivanje svakog narednog odbrambenog „prstena“ zahteva više napora i vremena. Po pravilu, kako se ide od spoljašnjeg prema unutrašnjim krugovima zaštite, sadržaj je vredniji i samim tim i sredstva zaštite su koncentrisanija, dok se sa druge strane nadzirani prostor smanjuje, pa je zaštita pouzdanija. Za ovakav pristup se u literaturi često koristi termin „zlatni broj sedam“ čime se ukazuje na to da treba uspostaviti sedam odbrambenih „prstenova“ da bi se postigao najviši nivo bezbednosti, slika 25.1.

Sedam odbrambenih prstenova - „linija obrane“ čine:

1. linija perimetra (sa ili bez fizičkih barijera),
2. prostor između perimetra i objekata u kompleksu,
3. granica objekta (zidovi),
4. otvori na objektu (vrata, prozori, razni otvori),
5. unutrašnje pregrade,
6. neposredna okolina cilja,
7. cilj - razlog neovlašćenog ulaska (krajnja tačka prilaza).




**Slika 25.1 „Zlatni broj sedam“ - sedam odbrambenih prstenova**

Ovakav pristup zaštiti od provale nije samo logičan već je i racionalan. Naime, tehničkim sredstvima za zaštitu od provale moguće je realizovati zaštitu maksimalnog nivoa bezbednosti već na samoj liniji perimetra i neposredno iza nje, međutim, to ekonomski nije opravdano s obzirom na dužinu granične linije i površinu prostora koja se štiti.

Realizacija zaštite od provale korišćenjem koncentričnih odbrambenih prstenova ima još jednu veliku prednost koja se sastoji u podešavanju željenog nivoa zaštite u skladu sa promenom sadržaja i namene objekta. Definisanje nivoa zaštite predstavlja pitanje koje uvek izaziva dilemu zbog kriterijuma i preporuka na osnovu kojih se vrši gradacija nivoa. Naime, sadržaj ili materijalna vrednost kao kriterijum za definisanje zaštite je veoma relativan faktor zato što na primer, informacija koja je sadržana u predmetu može da ima mnogo veću vrednost od samog predmeta (podaci na hard disku računara mogu više da vrede od samog računara). Zbog toga je pogodnije da se nivoi zaštite definišu u skladu sa *efektima* koji se njime postižu u smislu odvraćanja i sprečavanja neovlašćenog ulaska u pojedini odbrambeni prsten. U skladu sa takvim pristupom, definišu se *pet nivoa* zaštite:

1. Nivo - *minimalna zaštita*. Najniži nivo zaštite u tehničkom i materijal-nom pogledu. Neovlašćeni pristup se sprečava fizičkim barijerama, ogradama, vratima i prozorima od standardnog materijala i sa običnim bravama. Ovo je najčešći nivo zaštite koji se primenjuje kod stambenih zgrada i na javnim objektima.
2. Nivo - *nizak nivo zaštite*. Prvi nivo zaštite koji uključuje detekciju i lokalno alarmiranje korišćenjem jednostavnih alarmnih sistema, sa ili bez komunikacije sa višim nivoom nadzora (policija, službe obezbeđenja). Mehanička zaštita uključuje vrata i prozore sa ojačanjima, rešetkama i slično. Ovaj nivo zaštite se najčešće primenjuje u privatnim kućama, manjim trgovinama, ekspoziturama banaka, itd.
3. Nivo zaštite - *srednji nivo zaštite*. Koristi jednostavnije alarmne sisteme čija je uloga detekcija neovlašćenog pristupa na graničnoj liniji zaštite i delimično u unutrašnjosti zone koja se štiti. Ovaj nivo uključuje obavezno daljinsko alarmiranje, tj. komunikaciju sa višim nivoom nadzora i postojanje službe fizičkog obezbeđenja. Najčešće se primenjuje kod zaštite banaka, muzeja, velikih trgovina i slično.
4. Nivo zaštite - *visok nivo zaštite*. Ovaj nivo zaštite omogućava sprečavanje, otkrivanje i procenu neovlašćenog pristupa na liniji perimetra, u unutrašnjem prostoru i u samim objektima. Osim primene komponenti koje postoje na nivou tri u većem obimu, ovaj nivo uključuje i sistem za kontrolu pristupa (identifikacione kartice, sistem biometrije i sl.), sistem zatvorenog video nadzora i dobro organizovanu i obučenu sopstvenu službu fizičkog obezbeđenja. Ovaj nivo zaštite se primenjuje za zaštitu objekata od velikog značaja - materijalnog, društvenog, proizvodnog, itd.
5. Nivo zaštite - *maksimalna zaštita*. Ovaj nivo podrazumeva kompletnu zaštitu spolja i unutra primenom svih komponenti koje ima nivo četiri, s tim što je sistem najčešće deo integrisanog sistema zaštite sa lokalnim i daljinskim nadzorom pomoću komunikacionih mreža različite prirode (Intranet, Internet, sopstvena računarska mreža sa satelitskim linkom i slično). Ovaj nivo zaštite je najređi u praksi i primenjuje se kod kompleksa koji su od posebnog strateškog i društvenog značaja.

Razvoj tehnologije, pre svega elektronike, je značajno izmenio karakteristike i mogućnosti sistema za zaštitu od provale, pre svega u smislu projektovanja sistema za zaštitu od provale prema specifičnim potrebama i namenama. Ključne komponente sistema se nisu promenile u smislu da sistem mora da sadrži detektore provale, centralnu jedinicu (alarmnu centralu) koja obrađuje podatke dobijene od senzora i generiše signal alarma, kao i komunikacionu strukturu koja omogućava prenos alarmnih informacija višim nivoima nadzora i upravljanja, ali su priroda i pouzdanost navedenih komponenti značajno poboljšane. Na drugoj strani, svi sistemi zaštite uključuju i ljudstvo (službu fizičkog obezbeđenja), i postupke i procedure koje imaju ako ne veću, bar istu važnost kao i sam sistem.

Da bi instalirani sistem za zaštitu od provale bio efikasan potrebna je odgovarajuća obučenost ljudstva ne samo u rukovanju sistemom, već i u reakciji na moguće pokušaje ulaska u prostor i objekte koji se štite. U većini primena, detektori provala se koriste zajedno sa različitim oblicima fizičkih barijera čija je uloga da spreče ulazak ljudi ili vozila u prostor koji se štiti. Definisanje prostora koji se štiti, izbor tipa detektora, kao i definisanje mogućih pretnji i „slabih tačaka“ sa aspekta provale, pred-stavljaju prve korake u projektovanju sistema za zaštitu od provale, a u isto vreme to su i osnovni elementi procedure procene rizika od provale koja prethodi projektovanju.

## 25.2 Polazne osnove projektovanja

Pre nego što se krene sa projektovanjem sistema za zaštitu od provale za konkretan objekat, potrebno je proceniti tri najznačajnije karakteristike budućeg sistema:

1. verovatnoću (mogućnost) detekcije,
2. stopu lažnih alarmiranja (smetnje i izvore lažnih alarma) i
3. „osetljivost“ sistema na pokušaje obilaženja ili izbegavanja detektora („pokrivenost“ objekta ili prostora).

**Verovatnoća detekcije** označava sposobnost detektora da otkrije ulazak ili kretanje u zoni koja je pod nadzorom i zavisi ne samo od karakteristika detektora već i okruženja, metoda za instaliranje i podešavanje detektora, kao i ponašanje potencijalnog „uljeza“. Iako se detektori provale projektuju ciljno za zaštitu od neovlašćenog pristupa u okolni prostor ili objekat, mnogi tipovi detektora provale mogu da se koriste i u jednom i u drugom okruženju.

Verovatnoća detekcije, odnosno pouzdanost detekcije (eng. *Probability of Detection*), nezavisno od tipa detektora koji se koriste u sistemu i mesta postavljanja, zavisi od šest faktora:

1. količina i karakteristike emitovane energije,
2. veličina objekta koji se kreće,
3. rastojanje od objekta koji se kreće,
4. brzina objekta koji se kreće,
5. pravac kretanja objekta,
6. karakteristike refleksije/apsorpcije energije od strane objekta koji se kreće i okruženja.

Teorijski, precizno definisani tip energije objekta, kao i veći, bliži i brži objekti imaju veću verovatnoću detekcije. Dalje, sporo kretanje u pravcu detektora ima manju verovatnoću detekcije od brzog kretanje upravno u odnosu na osu detektora. Najzad, veći kontrast između objekta koji se kreće i ukupnih karakteristika refleksije i apsorpcije ambijenta daju veću verovatnoću detekcije.

**Stopa lažnih alarma** označava očekivanu učestanost generisanja signala alarma koji nemaju poreklo u aktivnostima koje su vezane za neovlašćeni ulazak. I kod ovih sistema, kao i kod sistema za otkrivanje i dojavu požara, u zapadnoj literaturi se koriste dva pojma: smetnje (eng. *nuisance*) i lažni alarmi (eng. *false alarms*). Smetnje označavaju tip lažnog alarma čije poreklo je donekle ili potpuno poznato (kretanje životinja, elektromagnetne smetnje), dok se za lažne alarme ne zna poreklo, pa prema tome inicijalno mogu da se shvate kao stvarni alarm, ali za njih kasnija provera pokazuje da nije bilo pokušaja neovlašćenog ulaza u zonu koja se štiti. Međutim, kako se za većinu alarma ne može utvrditi uzrok neposredno po nastanku, potrebno je sve njih proveriti i sprovesti odgovarajuće postupke kao odgovor.

**Osetljivost** sistema na izbegavanje zona pokrivanja je takođe mera efikasnosti detektora pošto nijedan tip detektora ne može da detektuje sve moguće načine ulaska. Zato se potencijalne „slabe tačke“ sistema u kojima može doći do izbegavanja detekcije, obezbeđuju tako što se za pokrivanje koristi više detektora istog tipa i/ili više detektora različitog tipa da bi se postiglo preklapanje zona detekcije, kao i međusobna zaštita detektora od onesposobljavanja na bilo koji način.

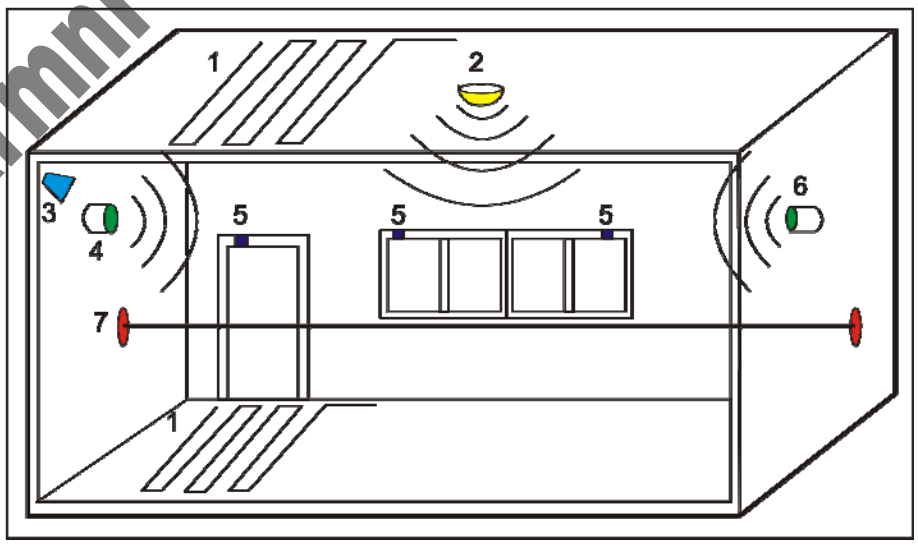
Većinu zona koje se štite karakteriše jedinstven skup ambijentalnih faktora koji moraju da se uzmu u obzir prilikom projektovanja sistema. Ukoliko se ne uzmu u obzir svi faktori okruženja posledice mogu da budu velika stopa lažnih alarma i postojanje „rupa“ u sistemu. Svi potencijalni prostori i mesta ulaska, bilo da se radi o perimetru i glavnom ulazu u kompleks, ili o vratima i prozorima na objektu, imaju karakteristične ambijentalne parametre koje je potrebno uzeti u obzir prilikom projektovanja.

Na primer, prilikom projektovanja zaštite prostora najznačajniji faktori koje treba uzeti u obzir su standardni klimatski uslovi tokom godine, dnevna fluktuacija temperature, aktivnosti zaposlenih i tehnološki procesi koji mogu da stvore uslove za alarmiranje, kao i kretanje životinja, vozila, vazdušna strujanja, itd. Ako se koristi ograda za odvajanje štićenog od okolnog prostora, ona mora da bude dobro konstruisana i učvršćena da ne bi svojim kretanjem pri vetrovitom vremenu izazivala alarmiranje. Dalje, prostor koji se štiti bi trebalo podeliti u alarmne sektore i zone da bi indikacija alarmiranja bila što preciznija i samim tim i brža reakcija službe obezbeđenja.

Slična razmatranja treba sprovesti i kada je u pitanju projektovanje sistema za zaštitu u okviru objekta. Osim uzimanja u obzir unutrašnjih ambijentalnih faktora (koji su kontrolisani i samim tim stabilniji), kao što su vazdušna strujanja i promene temperature kao posledica rada ventilacije i klima uređaja, treba uzeti u obzir i delovanje spoljnih faktora koji mogu da se prenesu u unutrašnjost, pre svega buke i vibracija kao posledica rada mašina ili ljudskih aktivnosti.

Bez obzira na to koliko dobro je projektovan sistem za zaštitu od provale, najslabija tačka svakog sistema je svakako napajanje. Veliki broj sistema nema mogućnost automatskog restartovanja sistema posle prekida i ponovnog uspostavljanja napajanja, već je potrebno da to uradi prisutno osoblje; takođe, prekid napajanja je jedan od metoda kome pribegava „uljez“ kod sistema kod koga proceni da je izuzetno pouzdan u smislu zaštite. Zbog toga je potrebno prilikom projektovanja predvideti rezervno - akumulatorsko napajanje svih vitalnih komponenti sistema: detektora, alarmne centrale, uređaja za uzbunjivanje i komunikaciju prema višim nivoima nadzora. Kapacitet rezervnog napajanja zavisi od sistema, ali je generalna preporuka da u slučajevima gde ne postoji služba za otklanjanje kvarova, rezervno napajanje treba da obezbedi rad sistema najmanje 72 h u bezalarmnom stanju sistema i bar 30 min rad uređaja za signalizaciju tokom trajanja alarmnog stanja.

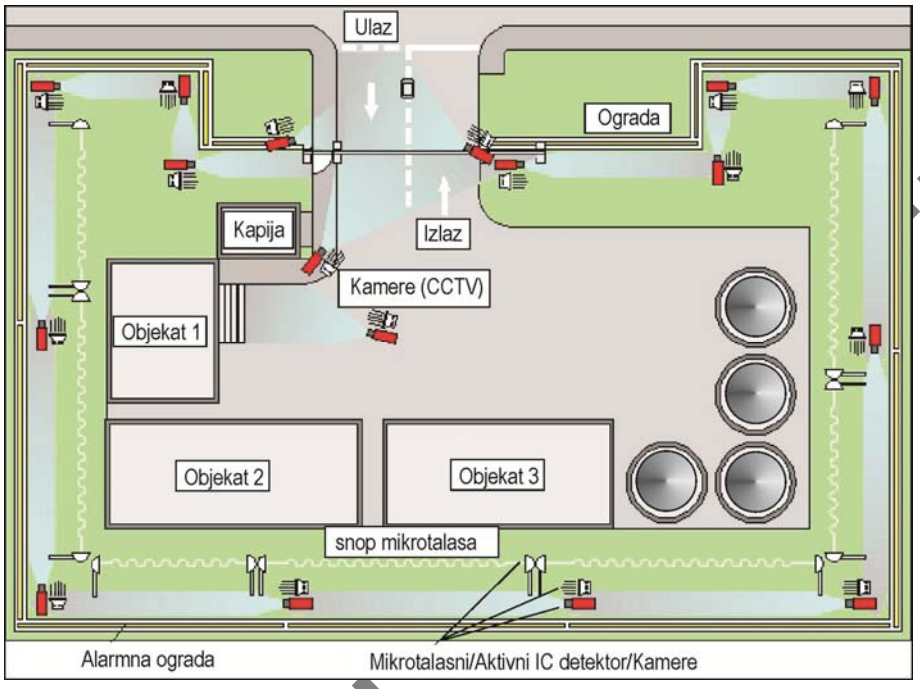
Na slici 25.2 su prikazani neki mogući tipovi detektora koji se mogu iskoristiti za nadgledanje prostorije, pri čemu tip detektora koji će biti upotrebljen, njihov broj i raspored zavisi od konkretne primene.




**Slika 25.2** Primer zaštite od provale u objektu

Značenje oznaka na prethodnoj slici je sledeće: 1 - optički kablovi u podu/plafonu, 2 - detektor pokreta (mikrotalasni, pasivni infracrveni, ultrazvučni), 3 - video detekcija pokreta, 4,6 - detektori vibracija, 5 - alarmni kontakti na vratima/prozorima (magnetni kontakt, mikroprekidač) i 7 - aktivni infracrveni detektor

Na sličan način se pristupa zaštiti perimetra i zaštiti prostora. U tu svrhu mogu da se iskoriste ne samo detektori, već i fizičke barijere (prirodne i veštačke), sistem video nadzora, sistem kontrole pristupa (kartični sistem, biometrija i slično), kao i redovni obilazak - patroliranje pripadnika službe fizičkog obezbeđenja, slika 25.3.




**Slika 25.3 Primer zaštite perimetra**

*Na liniji perimetra su pored bistatičkih mikrotalasnih detektora pokreta iskorišćeni aktivni infracrveni detektori pokreta iza alarmne ograde, koja može da se realizuje na bilo koji od opisanih načina zaštite perimetra. Zavisno od površine prostora koji se štiti, od lokacije objekata u okviru prostora i od njihovih građevinsko-arhitektonskih karakteristika, detektori koji su iskorišćeni za zaštitu perimetra mogu da se nađu i unutar tog prostora. To takođe važi i za sistem video nadzora, koji predstavlja neizostavni vid zaštite za velike komplekse.*

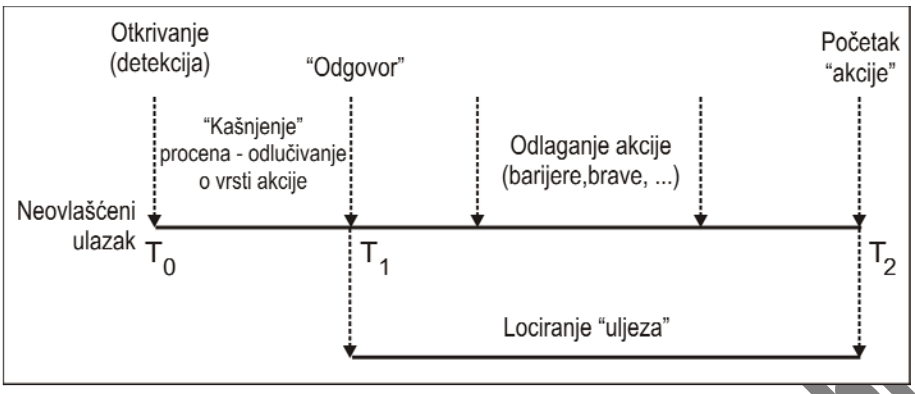
## 25.3 Metodologija projektovanja sistema

Bez obzira na to da li se radi o zaštiti perimetra ili o zaštiti objekata od neovlašćenog ulaska, proces realizacije zaštite od provale prolazi kroz tri faze: detekcija - kašnjenje - akcija. (Ovaj proces je poznat u zapadnoj literaturi kao *detect - delay - respond*):

- *detekcija* neovlašćenog ulaska u prostor/objekta (vreme otkrivanja ulaska),
- *kašnjenje* - vreme od upada do dolaska do cilja u objektu (vreme potrebno za odlučivanje o vrsti akcije),
- *odgovor/akcija* vreme koje je potrebno da služba fizičkog obezbeđenja sprovede odgovarajuće mere.

U fazi detekcije neovlašćenog ulaska, generisanjem signala alarma odmah ili neposredno posle otkrivanja, generiše se signal alarma kojim se obaveštava služba obezbeđenja o alarmnoj situaciji. Fazu detekcije prati procena o obimu i aktivnostima koje se dešavaju u štićenom prostoru i ta procena je najčešće potpomognuta informacijama dobijenim od sistema video nadzora ili obilaskom lokacije, posle čega sledi interno obaveštavanje ovlašćenih lica. Postojanje unutrašnjih barijera u prostoru ili prepreka u objektu produžava vreme dolaska „uljeza“ do cilja

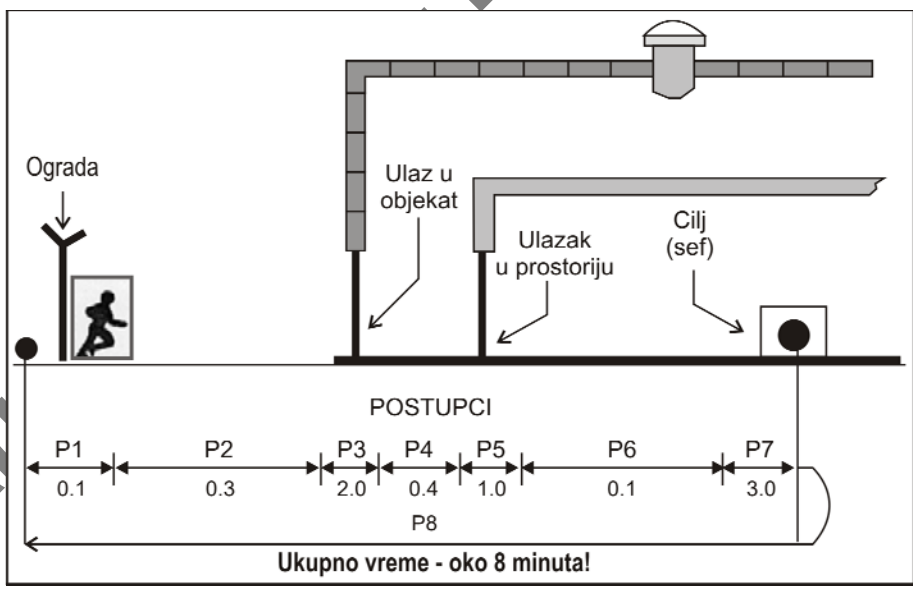
čime se daje dodatno vreme službi obezbeđenja za organizovanje uspešnijeg odgovora/akcije. Najzad, dolazi do akcije službe obezbeđenja kojom se uspostavlja kontrola nad prostorom koji se štiti i sistem se vraća iz alarmnog u normalno stanje, slika 25.4.




**Slika 25.4 „Scenario" organizacije sistema za zaštitu od provale**

Vreme između navedenih faza direktno utiče na efikasnost zaštite i predstavlja ukupno vreme reakcije sistema. Drugim rečima, simulacija funkcionisanja sistema zaštite uz pomoć računara ili u realnim uslovima može značajno da poboljša efikasnost zaštite.

Na slici 25.5 je prikazan primer mogućeg redosleda događaja (scenario) ulaska u kompleks koji se štiti, sa definisanim vremenima pojedinih faza neovlašćenog ulaska od momenta detekcije do preduzimanja akcije. Scenario je napravljen tako da počinje prelaskom linije perimetra i završava se dolaskom do ciljanog predmeta (na primer, sef). S obzirom na činjenicu da služba obezbeđenja ne može da reaguje odmah po signalizaciji alarma, vremenski okvir koji je potreban da „uljez" pređe prostor od perimetra do objekta u kome se nalazi cilj upada je postavljen na 3 minuta, pri čemu se podrazumeva da je signal alarma generisan pri prelasku linije perimetra.



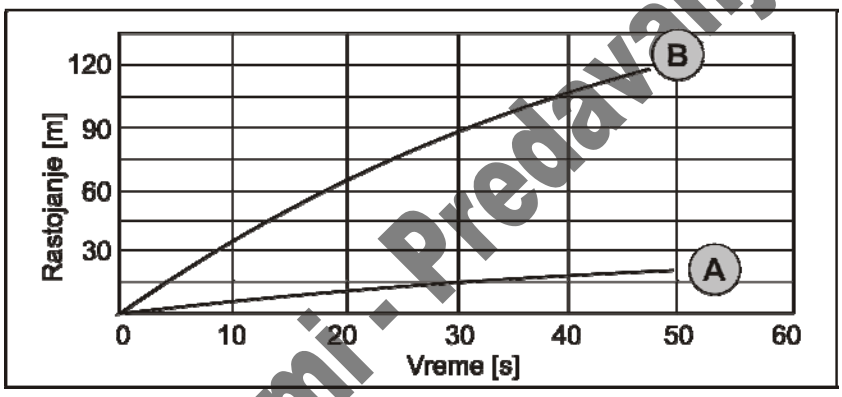

**Slika 25.5 Scenario ulaska u štićeni prostor**

Pravljenje ovakvog scenarija korišćenjem bilo kakvog načina simulacije je korisno za definisanje cilja zaštite. Na primer, ako je cilj da se „uljez" onemogući pre ulaska u sam objekat, služba obezbeđenja treba da locira uljeza i bude na licu mesta za manje od 2 minuta od momenta alarmiranja. Ako je cilj da se „uljez" uhvati „na delu" - to vreme bi bilo 6 minuta, a ako je cilj da se onemogući iznošenje ukradenog predmeta van kompleksa, vremenski okvir akcije je do 8 minuta od momenta alarmiranja. Vremena iskorišćena za simulaciju su data u tabeli 25.1.

**Tabela 25.1** *Potrebno vreme za savladavanje pojedinih prepreka od momenta detekcije*

| Postupak | Vreme [min] | Opis |
|---|---|---|
| P1 | 0.1 | *Prelazak ograde* |
| P2 | 0.3 | *Pretrčavanje 75 m* |
| P3 | 2.0 | *Prolazak kroz vrata* |
| P4 | 0.4 | *Prelazak 16 m* |
| P5 | 1.0 | *Obijanje brave* |
| P6 | 0.1 | *Dolazak do cilja* |
| P7 | 3.0 | *Otvaranje sefa* |
| P8 | 1.0 | *Uzimanje materijala i bekstvo* |
| Ukupno | 7.9 | Ukupno vreme boravka u prostoru |

Primer koji je prikazan na slici 25.5 i tabeli 25.1 može da posluži kao uzorak prilikom planiranja i izrade plana akcije u slučaju neovlašćenog ulaska. Ovo je pojednostavljeni primer, jer ako „uljez“ sa sobom nosi neki teret (najčešće alat za obijanje), prolazna vremena su značajno veća. Na slici 25.6 su prikazana srednja vremena kretanja sa teretom - penjanje uz stepenice i trčanje, tako da prikazane krive mogu da pred-stavljaju polaznu osnovu prilikom izračunavanja vremena za akciju.



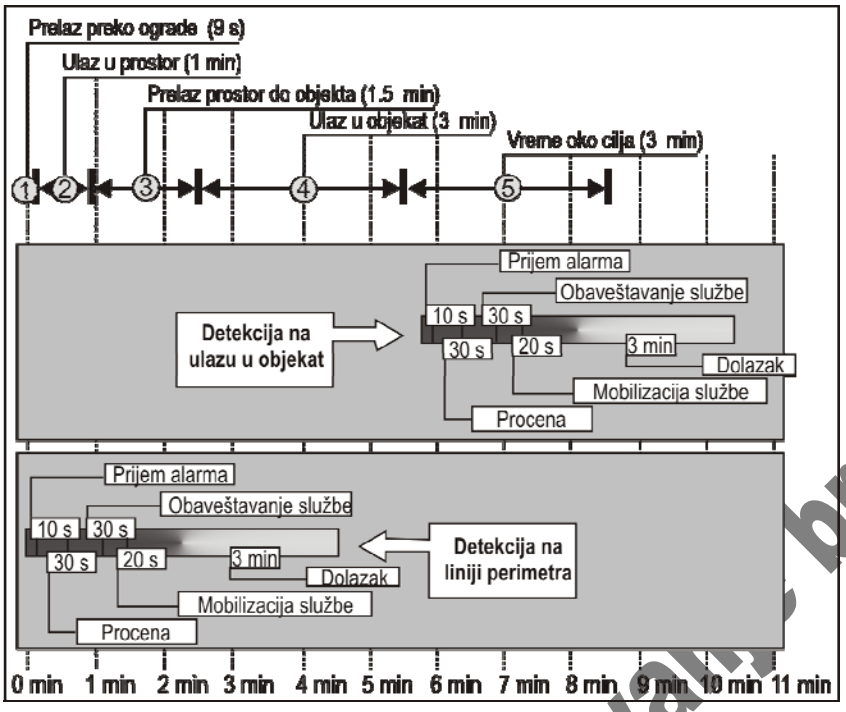

**Slika 25.6 Vreme prelaska i pređeni put sa teretom (alat težine 16 kg)**

*Oznake na slici: kriva A-penjanje uz stepenice, kriva B-trčanje na otvorenom prostoru.*

Pošto bi vreme izlaska na „teren“ službe fizičkog obezbeđenja trebalo da bude minimalno i poznato, scenario mogućeg ulaska u štićeni prostor može da se predstavi i pomoću vremenskog dijagrama koji će sadržati i podatke koji se odnose na vreme potrebno za preduzimanje akcije. Na slici 25.7 vremenskim dijagramima su ilustrovana dva moguća slučaja reakcije službe fizičkog obezbeđenja.

U prvom slučaju, alarmiranje se dešava tek kod ulaska u objekat u kome se nalazi cilj. Sa inicijalnim zakašnjenjem generisanja alarmnog signala od 6 minuta, služba fizičkog obezbeđenja će biti na mestu događaja tek posle 11 minuta od ulaska - najverovatnije kada je događaj već završen.

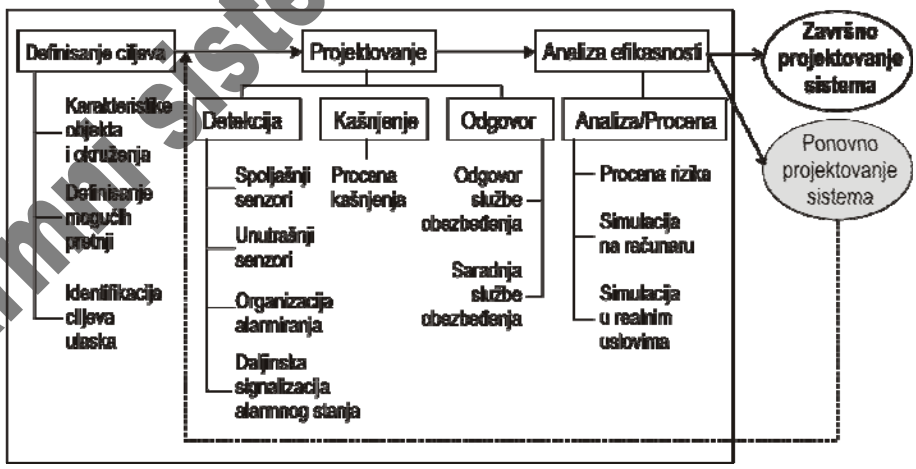
U drugom slučaju, šanse da se osujeti provala su znatno veće, jer je signal alarma generisan odmah po prelasku linije perimetra, što je omogućilo službi fizičkog obezbeđenja da stigne na lice mesta za manje od 6 minuta, pre pokušaja ulaska u objekat u kome se nalazi cilj provale.




**Slika 25.7 Scenario sa vremenskim dijagramom koji uključuje vreme potrebno za dolazak na mesto događaja**

*Ako do detekcije dođe već na samoj liniji perimetra, „uljez" će biti zatečen na delu; ako do detekcije dođe tek na ulazu u objekat, velika je verovatnoća da „uljez" neće biti onemogućen u zadatom vremenskom okviru od 8 minuta.*

Navedene činjenice su takođe ključne prilikom procesa projektovanja sistema za zaštitu od provale. Kao što se vidi sa slike 25.8, projektovanje sistema za zaštitu od provale predstavlja iterativni proces u kome se kao poslednji korak javlja analiza i procena efikasnosti sistema koja najviše zavisi upravo od karakteristika pojedinih faza realizacije zaštite od provale: detekcije, kašnjenja i odgovora.




**Slika 25.8 Postupci prilikom projektovanja sistema za zaštitu od provale**

Struktura sistema za zaštitu od provale, koja podrazumeva izabrani tip detektora, njihov broj i međusobni raspored, lokaciju centrale kao i komunikacione linije, zavisi najviše od zahteva koji se preciziraju u prvom koraku (definisanje ciljeva sistema). Ako se u ovom početnom koraku projektovanja naprave greške, veoma ih je teško kasnije ispraviti kada se sistem instalira, poveže i obezbedi odgovarajuća programska podrška. Zbog toga uvek treba

sačekati rezultate izvršenih simulacija i analiza pre nego što se izvrši konačno projektovanje sistema.

Da bi proces projektovanja kao rezultat dao pouzdan sistem za zaštitu od provale, potrebno je definisati/pretpostaviti što veći broj različitih scenarija neovlašćenog ulaska, na način opisan u ovom poglavlju, i te rezultate iskoristiti za procenu ukupne efikasnosti sistema koja će pokazati da li je potrebno ponovno projektovanje.

Najzad, dobro organizovan sistem za zaštitu od provale treba da poseduje sledeće karakteristike:

- Da poseduje funkcije i način alarmiranja (za ljude u obezbeđenju i za ostale) koje su jasne, razumljive, precizno opisane i brzo se prihvataju;
- Da bude u potpunosti komplementaran sa funkcijama sistema fizičke zaštite;
- Da bude jednostavan za instaliranje, rukovanje, održavanje, ali da sa druge strane bude efikasan;
- Da ne postoji mogućnost „zaobilaženja“ sistema, da ima dug radni vek bez otkaza, ili sa malom stopom otkaza i da bude zaštićen od diverzije spolja ili unutra;
- Da bude prihvatljiv za sve korisnike, bez obzira na razlike u nivou tehničkog obrazovanja;
- Da bude pouzdan i sa malom stopom lažnih alarma.

Da bi navedeni zahtevi bili ispunjeni, potrebno je da u procesu planiranja, projektovanja i organizacije sistema, učestvuju stručnjaci različitih profila čiji zahtevi će biti ispunjeni kroz tehničku realizaciju sistema.

## 26 Sistemi za kontrolu pristupa

Najjednostavniji, i najpouzdaniji način kontrole pristupa nekom prostoru van ili unutar objekta je *direktna kontrola pristupa* koja se realizuje aktivnostima fizičke službe obezbeđenja. Međutim, ovaj zadatak može da zahteva angažovanje velikog broja pripadnika službe obezbeđenja, jer zavisi ne samo od veličine prostora i objekta koji se štiti, već i od broja pristupnih tačaka – ulaza, sadržaja i procesa koji se odvijaju u objektu, potrebe da pojedini delovi i resursi štićenog prostora zahtevaju visok stepen zaštite, itd. Navedeni razlozi koji u pojedinim slučajevima nisu ekonomski opravdani, kao i uvek prisutna mogućnost ljudske greške, nameću upotrebu indirektne zaštite od neovlašćenog ulaska korišćenjem odgovarajuće elektronske opreme. *Indirektna kontrola pristupa* se obavlja, pre svega, ***sistemima za kontrolu pristupa*** koji se realizuju na dva načina: *kartičnim sistemom pristupa* i *sistemima biometrijske identifikacije*.

Kontrola pristupa u najširem smislu, podrazumeva nadzor nad pristupom određenim resursima, pod određenim uslovima i u određenom vremenskom periodu. Oblasti primene sistema za kontrolu pristupa kreću se od kontrole prava pristupa otvorenim i zatvorenim prostorima, evidencije ulaska i izlaska iz tih prostora, sve do kontrole pristupa pojedinim sredstvima i opremi sistema od značaja, kao što su informacioni sistemi, telekomunikaciona oprema i slično.

Razni oblici kontrole pristupa se i inače svakodnevno koriste, počev od „običnih“ vrata kod kojih je kontrola svedena na bravu i ključ, pa sve do raznih tipova sigurnosnih vrata sa posebno izrađenim ključevima. Međutim, ograničenje pristupa mehaničkim bravama se odnosi samo na lice koje ulazi (lice mora da poseduje ključ) i mesto ulaska (lokacija vrata u odnosu na resurs koji se štiti), a ne i na vreme i trajanje pristupa. Osim toga, osnovni problem kod mehaničkih brava je nedostatak autorizacija pristupa, jer ključ može da se izgubi i da dođe u posed drugog lica ili da se jednostavno pozajmi drugom licu. Zbog toga je neophodna *elektronska kontrola pristupa* kojom se prevazilaze ograničenja koja poseduju mehaničke brave i ključevi.

Suština elektronske kontrole je u dozvoli pristupa na osnovu dodeljenih ovlašćenja. Drugim rečima, ako su vrata u pitanju, kada je pristup odobren, vrata su otključana unapred određeno vreme, a podaci o licu i vremenu pristupa su zapamćeni. Kada je pristup odbijen, vrata ostaju zaključana i pokušaj pristupa je zabeležen. Sistem će takođe ispratiti sve dozvoljene pokušaje (najčešće tri) i aktivirače alarm posle sledećeg pokušaja ili u slučaju nasilnog otvaranja vrata, kao i u slučaju kada se vrata drže otvorena predugo posle otključavanja.

Nivo i složenost kontrole pristupa zavisi i određuje se u skladu sa značajem resursa koji se štiti, ali svaki sistem za kontrolu pristupa treba da realizuje sledeće tri funkcije koje se obavljaju sekvencijalno, jedna za drugom:

- identifikacija,
- verifikacija i
- autorizacija

*Identifikacija* podrazumeva proces dobijanja različitih informacija od lica koje pristupa (korisničko ime, broj računa i slično) pomoću kojih se lice identifikuje.

*Verifikacija* podrazumeva proveru identiteta lica koje se identifikovalo u prethodnom koraku tako što se od lica zahtevaju dodatne informacije, kao što je lozinka, PIN kôd i slično. Postoje tri osnovna načina provere na osnovu kojih može da se obavi verifikacija:

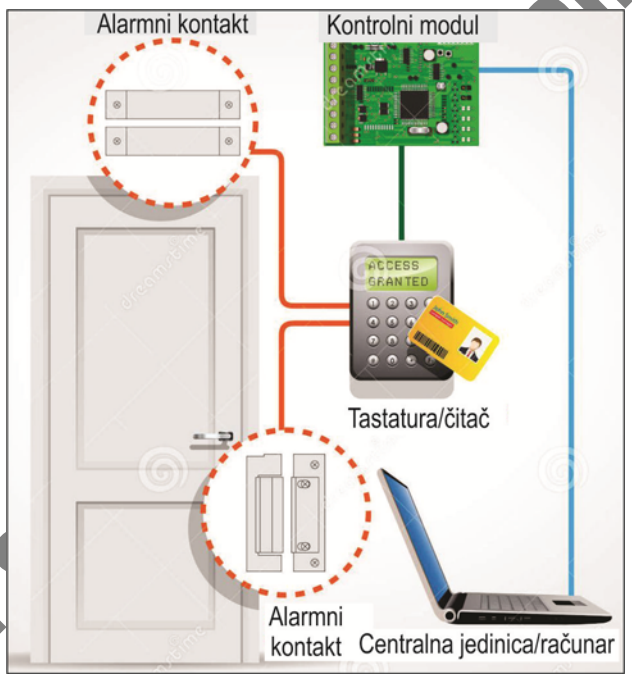
- na osnovu informacije da korisnik nešto zna – lozinka
- na osnovu nečega što korisnik poseduje – kartica i
- na osnovu informacije ko je korisnik – biometrijskim proverama.

Autorizacija predstavlja proces dodeljivanja „prava pristupa“ ili nivo ovlašćenja licu na taj način što se na osnovu prethodno dobijenih podataka licu omogućava pristup u određeni prostor ili operacije koje može da izvrši na određenoj opremi. Zavisno od nivoa ovlašćenja i važnosti

resursa kojima se pristupa, autorizacija može da se zasniva na jednoj ili na sve tri prethodno navedene provere. Na primer, kolega može da pozajmi svoju karticu drugom kolegi, da mu kaže svoju lozinku, itd., ali konačna dozvola pristupa će biti omogućena posle biometrijske provere.

Imajući u vidu da je tačka pristupa koja se kontroliše ulaz, koji može biti u formi vrata, rampe ili bilo koje fizičke barijere, sistemi kojima se realizuje kontrola pristupa uglavnom sadrže sledeće komponente:

- Nezavisna *elektronska brava* koja se standardno otključava od strane dežurnog prekidačem. U sistemu za kontrolu pristupa ona se zamenjuje *čitačem*.
- *Čitač* može da bude tastatura za unošenje koda, *čitač kartica*, ili *biometrijski čitač*. Uloga čitača je da prosledi uneti kôd centralnoj jedinici (kontrolnom modulu sistema) koja obavlja proveru da li se kôd nalazi u spisku dozvoljenih šifri. U slučajevima gde je izlaz takođe pod kontrolom, koristi se još jedan čitač na drugoj strani vrata.
- Dodatne komponente, kao što je *alarmni kontakt* za praćenje pozicije u kojoj se nalaze vrata ili neki od tipova detektora provale. A primer, može se iskoristiti i *detektor pokreta* u slučajevima u kojima se ne kontroliše izlaz, mada je to jednostavnije realizovati običnim tasterom za otvaranje vrata. Pri izlasku, alarm se privremeno isključuje dok su vrata otvorena i to može biti slaba tačka ovog sistema.




**Slika 26.1 Ilustracija kontrole pristupa**

## 26.1 Čitači kartica

Čitači kartica predstavljaju ključnu komponentu sistema sa osnovnim zadatkom da učitaju podatke koji se nalaze na kartici, da podatke proslede kontrolnom modulu ili centralnoj jedinici, i eventualno, da izvrše obradu tih podataka. Čitači se obično klasifikuju u tri kategorije u skladu sa opsegom funkcija koje obavljaju:

1. "*Obični*" čitači, ili tzv. *neinteligentni* čitači čija je uloga da pročitaju broj kartice ili PIN i da ga proslede centralnoj jedinici (centrali). U slučaju biometrijske identifikacije ovi čitači prosleđuju ID broj korisnika. Prenos podataka se obavlja bežičnim (wifi) prenosom ili korišćenjem standardnog naponskog ili strujnog protokola (RS232 i RS485).
2. *Poluinteligentni* čitači osim funkcije čitanja i prosleđivanja podataka koji se nalaze na kartici poseduju funkcije koje su potrebne za kontrolu ulaza i izlaza na taj način što kontrolišu

potrebne komponente za to (bravu, kontakt na vratima, izlazni taster), ali ne odlučuju o dozvoli pristupa. Kada korisnik predstavi svoju karticu ili unese PIN, čitač šalje podatke na glavni kontroler i čeka odgovor. Za vezu sa kontrolnim modulima se obično koristi strujna, RS-485 komunikacije.

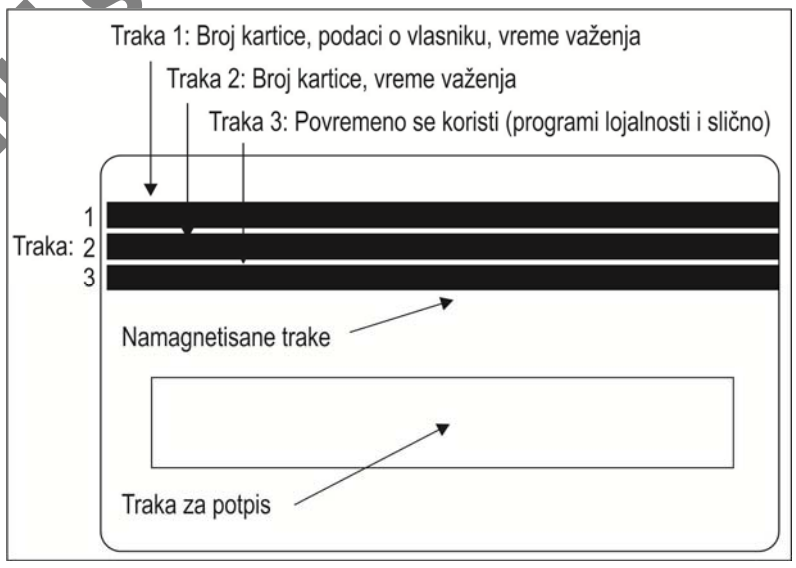
3. *Inteligentni* čitači pored funkcija koje poseduju prethodna dva tipa čitača, mogu da donose odluku o dozvoli pristupa zahvaljujući dodatnom hardveru koji podrazumeva upotrebu mikrokontrolera ili mikroprocesora. Savremeni inteligentni čitača imaju mogućnost povezivanja na lokalnu računarsku mrežu u kojoj im se dodeljuju jedinstvena IP adresa, tako da se nazivaju i „IP čitači". Zahvaljujući tome, oni ne moraju da se povezuju na kontrolni modul, već direktno komuniciraju s računarom koji vrši kompletnu obradu podataka. Zavisno od upotrebljenog hardvera, neki čitači mogu da imaju i tastaturu, ugrađenu kameru, mikrofon i zvučnik za interfon, itd.

## 26.2 Identifikacione kartice

Uloga identifikacionih kartica u zaštiti od neovlašćenog ulaska ili pristupa pojedinim delovima prostora i objekta nije samo u tome da se prikupe osnovni podaci o licu koje ulazi, već i da se dodeli unapred definisan nivo pristupa. Sistemi za kontrolu pristupa najčešće koriste četiri tipa kartica:

- *Kartice sa magnetnom trakom* (eng. *magnetic strip*);
- *Kartice za udaljenu identifikaciju* (eng. *proximity cards*);
- *„Pametne" kartice* (eng. *smart cards*) i
- *Kartice u dualnoj tehnologiji* (eng. *dual technology cards*).

*Kartica sa magnetnom trakom* koja se nalazi na poleđini kartice sadrži informacije o licu koje zavise od tipa kartice i prostora ili objekta za koje važe, kao i dozvoljeni nivo pristupa. Ovaj tip kartica se najčešće sreće u svakodnevnom životu i primenjuje se u najrazličitijim oblastima, počev od kartica za ličnu identifikaciju (lične karte), preko banaka (bankomata) za podizanje novca, u hotelima za otključavanje prostorija, u tržnim centrima, itd. Ovaj tip kartica je našao široku primenu pre svega zbog niske cene i mogućnosti da sadrže alfanumeričke podatke. Takođe, ovaj tip kartica se lako individualizuje štampanjem u različitim bojama ili dodavanjem fotografije ili nekog simbola na njih. Osnovna mana im je što se lako oštećuju, prljanjem ili mehanički, u blizini spoljašnjeg magnetnog polja, a za pojedine tipove kartica je lako napraviti duplikat. Sastavni deo sistema su i čitači kartica koji se projektuju posebno za svaku primenu.




**Slika 26.2 Kartica sa magnetnom trakom**

*Kartice za udaljenu identifikaciju* omogućavaju identifikaciju na malom rastojanju od uređaja za čitanje, bez ubacivanja kartice u sam uređaj. Da bi se obavilo prijavljivanje ovim karticama dovoljno je da se približi na trenutak jedinici elektronskog čitača. Čitač proizvodi zvuk kojim oglašava karticu pročitanom. Za ove kartice postoji predviđen okvirni prostor od 5 cm za očitavanje, tako da korisnik ovakvu karticu može držati u džepu, novčaniku ili torbi, i za očitavanje je dovoljno da ih približi čitaču. U odnosu na kartice sa magnetnom trakom, ove kartice mogu sadržati veću količinu podataka, i mogu se koristiti i u svrhe sistema beskontaktnog plaćanja.

Postoje dva tipa ovih kartica. Prvi tip kartica koristi programibilni čip koji ima jedinstveni pristupni kod i integrisanu antenu koja radi na frekvenciji od 125 kHz. Drugi tip kartica se zasniva na upotrebi tzv. *Wiegand* tehnologije koja je nazvana po fizičaru J. R. Wigandu koji je otkrio nelinerni magnetni efekt koji proizvode na poseban način kaljene žice od legure kobalta, čelika i vanadijuma. Kod ovog tipa kartice koriste se provodnici veoma malog prečnika koji su umetnuti u traku na kartici u dva reda. Broj kodova na kartici zavisi od broja provodnika koji su sačinjeni od posebne feromagnetne legure, njihovog redosleda i međusobnog rastojanja između provodnika.


**Slika 26.3 Kartica za udaljenu identifikaciju**

*„Pametne" kartice* sadrže programibilni čip što omogućava sa jedne strane, da sistem za kontrolu pristupa menja sadržaj informacija koje se nalaze na kartici na osnovu svoje baze podataka i, sa druge strane, da informacije koje se nalaze na kartici budu različite po količini i prirodi. Ove kartice se izrađuju kao kontaktne i kao bezkontaktne kartice u odnosu na čitač kartica. Bezkontaktne smart kartice koriste *wireless* tehnologiju (rade na 13.56 MHz) što znači da omogućavaju više od sto puta veći protok podataka nego standardne kartice sa udaljenim pristupom. Ovaj tip kartica je veoma pouzdan u radu i omogućava pamćenje velikog broja podataka.


**Slika 26.4 Programibilni čip pametne kartice**

*Kartice u dualnoj tehnologiji* se realizuju korišćenjem dve različite tehnologije, a najčešća kombinacija je magnetna traka i udaljena identifikacija.

## 26.3 Organizacija kontrole pristupa

Organizacija zaštite od neovlašćenog pristupa korišćenjem kartica za identifikaciju se realizuje u nekoliko koraka. U prvom koraku je potrebno definisati delove prostora ili objekta u kojima je potrebno obavljati identifikaciju. Ponekad je dovoljno da se ograniči pristup samo na stepeništima ili hodnicima koji vode u delove objekta koji su od posebne važnosti. Prilikom definisanja delova kod kojih se primenjuje kontrola pristupa, za svaki od njih treba definisati tri osnovne karakteristike:

- potpuni pristup koji se kontroliše u nekoliko pristupnih tačaka,
- ograničenja u pristupu i
- izuzetke od kontrole pristupa.

Definisanje potpunog pristupa podrazumeva kontrolu nad svima koji se nalaze u tom delu objekta i kombinuje se sa ograničenjima u pristupu za pojedine delove objekta, na primer, laboratorije u istraživačkom centru, centralni računarski centar i slično. Izuzeci mogu da se odnose na prostorije opšte namene, kao što su bifei, sanitarne prostorije ili prostori namenjeni za prolaz ljudi ili robe u objektu. Takođe, veoma je važno da se definiše potreban broj tačaka - ulaza za kontrolu pristupa tako da u vremenu najveće gužve (na primer, dolaska na posao ili odlaska sa posla) sam proces kontrole ne traje predugo.

Kada se definišu restriktivna područja u prostoru ili objektu sa definisanim nivoima pristupa, ograničenjima i izuzecima, kao i pristupne tačke, u sledećem koraku se bira tip kartice, tj. primenjena tehnologija. Na primer, ako se koristi 32-bitna kartica, izdvaja se određeni broja bitova za broj kartice (broj korisnika) i određeni broj bitova za informaciju o korisniku. Taj odnos je kod ovih sistema najčešće 16 + 16 bitova, što daje mogućnost kontrole ogromnog broja korisnika i pamćenja velike količine podataka za svakog od njih.

Osnovna prednost kartičnih sistema pristupa je u tome što su veoma pouzdani, imaju dug period eksploatacije sa malim troškovima održavanja. Osnovna mana je u tome što kartice mogu da se izgube ili da budu ukradene, a moguće je napraviti duplikat nekih tipova kartica.

Najzad, tehnologija koja se koristi za realizaciju pametnih kartica može biti upotrebljena i u formi klasičnog ključa koji sadrži programibilni čip sa bravom koja sadrži čitač kartice, čime se mehanički način zaštite kombinuje sa tehnologijom sistema za kontrolu pristupa.


**Slika 26.5 Kombinacija mehaničke zaštite i tehnologije „pametnih“ kartica**

## 27 Sistemi za biometrijsku identifikaciju

Sistemi koji koriste biometrijske karakteristike za identifikaciju osoba koriste sledeće tipove uređaja za tu namenu:

- *Čitače otiska prsta* (eng. *fingerprint reader*);
- *Čitače otiska šake* (dlana), (eng. *hand geometry readers*);
- *Čitače dužice oka* (eng. *iris scanner*);
- *Čitače mrežnjače oka* (eng. *retina scanner*);
- *Uređaje za prepoznavanje glasa* (eng. *voice recognition*);
- *Uređaje za prepoznavanje lica* (eng. *facial recognition*).

Biometrija se može definisati kao model identifikacije osobe, koji je baziran na fizičko-fiziološkim karakteristikama ili karakteristikama ponašanja, a neki autori daju opštiju definiciju u smislu da se biometrija bavi identifikacijom pojedinaca, koja je zasnovana na biološkim karakteristikama osobe. U samim počecima realizacije i upotrebe biometrijskih sistema, fizičke karakteristike su imale prednost u odnosu na karakteristike ponašanja, tj. preovladavalo je uverenje da su fizičke karakteristike pouzdanije, jer imaju tendenciju da se manje menjaju u odnosu na karakteristike ponašanja. Metodi biometrije danas se koriste pri izradi identifikacionih dokumenata, autorizaciji ulaska i kretanja u okviru perimetra i u objektima, a u novije vreme sve više i za identifikaciju osoba.

Klasični (jednokriterijumski) biometrijski sistemi koriste samo jedan metod za identifikaciju osobe. Iako su zbog toga jednostavniji za primenu, sa brojem ljudi koji se kontrolišu raste i mogućnost greške. Na primer, među dovoljno velikim brojem ljudi lako je pronaći dve osobe sa veoma sličnim licem. Biometrijski sistem se može zasnivati i na većem broju biometrijskih osobina (više snimaka jedne biometrijske osobine) čime se dobija višekriterijumski (multimodalni) biometrijski model. Pošto se rad klasičnih bimetrijskih sistema zasniva na proveri samo jedne karakteristike, potrebno je da ta karakteristika bude jedinstvena, u smislu da ne dozvoljava „prevaru“ sistema. U tu grupu karakteristika mogu se ubrojati otisak prsta, dužica oka, mrežnjača oka i DNK. Navedenim karakteristikama je zajedničko to što se ne menjaju vremenom (starenjem osobe), ali i relativno dugo vreme koje je potrebno za obradu podataka. Kvalitetan klasičan biometrijski sistem se može poboljšati korišćenjem drugih biometrijskih karakteristika koje osoba poseduje, ali pomoću njih nije moguće sa potpunom pouzdanošću razlikovati osobe (visina, težina, pol, boja kose i slično). Nedostaci klasičnih biometrijskih sistema u odnosu na višekriterijumske biometrijske sisteme se najviše ogledaju u nivou primene, tj. u nivoima zaštite koju pružaju. Naime, višekriterijumski sistemi pružaju različite nivoe zaštite zbog toga što koriste dva ili više metoda za identifikaciju, čime pokrivaju široki spektar karakteristika osobe.

Višekriterijumski biometrijski sistemi u praksi kombinuju fizičke karakteristike i biometriju ponašanja i najčešće se kombinuju sa standardnim metodima zaštite i alarmnim sistemima, čime se minimizira mogućnost zloupotrebe. Na primer, ukoliko se koristi samo jedna tehnika kao što je prepoznavanje otiska prsta, tada je moguća situacija u kojoj neka osoba poseduje lažni otisak prsta kojim obavlja identifikaciju u ime neke osobe. Korišćenjem dodatnih biometrijskih karakteristika koje je teško falsifikovati, kao i drugih metoda za kontrolu pristupa, pouzdanost sistema zaštite se značajno povećava.

Fizičke karakteristike osobe koje mogu da se koriste za biometrijsku identifikaciju su otisak prsta ili šake, karakteristike oka i lica, pa čak i miris tela. Osim toga, za identifikaciju može da se koristi glas, način kretanja osobe, način kucanja na tastaturi računara, ili kako osoba odgovara na skup nekih pitanja. Najpouzdanija jedinstvena identifikacija je korišćenjem DNK, ali je to invazivan proces koji zahteva uzimanje uzorka ćelija kože ili krvi, tako da se još uvek ne primenjuje u zaštiti od provale.

Počeci biometrijske identifikacije se vezuju za kraj XIX veka, ali je tek kasnih 90-tih godina prošlog veka razvoj tehnologije omogućio masovniju upotrebu biometrijskih sistema.

*Čitači otiska prsta* analiziraju otisak prsta i upoređuju dobijenu sliku sa slikom u bazi podataka. Smatra se da su uređaji ovog tipa najzastupljeniji, statistički čine skoro 80% svih prodatih biometrijskih uređaja i njihov nivo greške je manji od 1%.

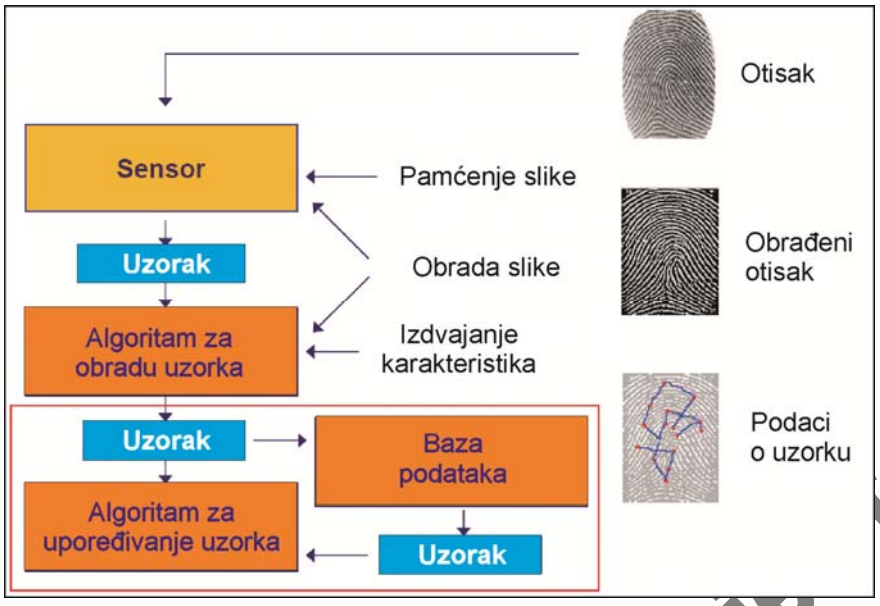

**Slika 27.1 Karakteristike otiska prsta**

Iz očitanih slika otisaka različitim metodama se izvlače uzorci. Na slici 27.1 su prikazane neke karakteristične tačke na otisku. Metodom analize pojedinosti analiziraju se relativni položaji individualnih karakteristika otiska kao što su završeci grebena, bifurkacije (mesta na kojima se dve linije spajaju u jednu), vrlo kratke linije i mesta gde se dve linije ukrštaju.

Metod analize pojedinosti, koji je preovlađujući u identifikaciji ovim metodom, ima nedostatak jer ne uzima u obzir čitavu strukturu otiska, već samo položaj i smer karakterističnih tačaka. Ovaj problem se može popraviti metodom korelacije kojim se upoređuje uzorak otiska u celini, međutim, osim činjenice da primena metoda na taj način zahteva značajno angažovanje računarskih resursa, položaj i zakrenutost prsta može značajno da utiče na pouzdanost metoda.

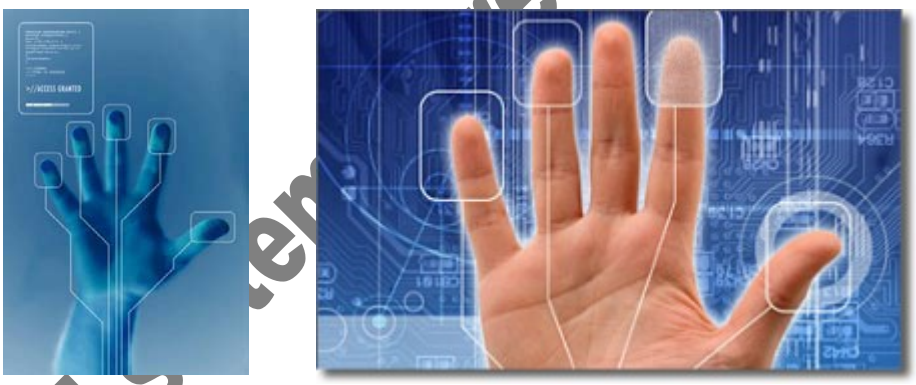
Najveći problem pri korišćenju otiska prsta za verifikaciju osobe jeste falsifikovanje otiska koje se najčešće obavlja pomoću tanke silikonske folije koja sadrži kopiju otiska druge osobe. Falsifikat se pravi bez neke naročite opreme i prilično lako se lepi na prst, tako da usavršavanje ovih uređaja u poslednje vreme ide u pravcu dodavanja senzora koji mere i neke druge osobine, kao što je provodljivost prsta, temperatura, puls i slično.

U svakom slučaju, biometrijska identifikacija korišćenjem otiska prsta je brza, tačna i izuzetno pouzdana. Čitači otiska prsta koji se danas koriste najčešće nemaju mogućnost poređenja otiska na hardverskom nivou, pa su zbog toga su jeftini i široko dostupni. Proces analize otiska prsta prikazan je na slici 27.2 i sa malim modifikacijama dobro ilustruje proces biometrijske identifikacije uopšte, nezavisno od primenjenog metoda.




**Slika 27.2** Ilustracija biometrijskog procesa identifikacije

*Čitači otiska šake (dlana)* analiziraju više od 31000 tačaka dlana i klasifikuju ih na osnovu 90 različitih kriterijuma. Merenja koja se obavljaju u čitaču uključuju širinu i dužinu šake, raspored linija na dlanu i druge karakteristike koje se upoređuju sa slikom šake koja se nalazi u bazi podataka. Procesu čitanja otiska prethodi identifikacija lica pomoću kartice, na osnovu čega se u bazi podataka pronalazi prethodno zapamćena slika šake za to lice.



**Slika 27.3** Biometrijsko ispitivanje geometrije dlana

Osim opisanog načina identifikacije, ispitivanje dlana može da se obavlja i na osnovu rasporeda, oblika i dubine kostiju, ili analizom rasporeda vena na šaci korišćenjem infracrvene kamere, odnosno, termografijom. Snimci dobijeni infracrvenom kamerom prikazuju položaj krvnih sudova dlana koji su jedinstveni za svakog čoveka.

**Slika 27.4** Biometrijsko ispitivanje kostiju i vena ruke

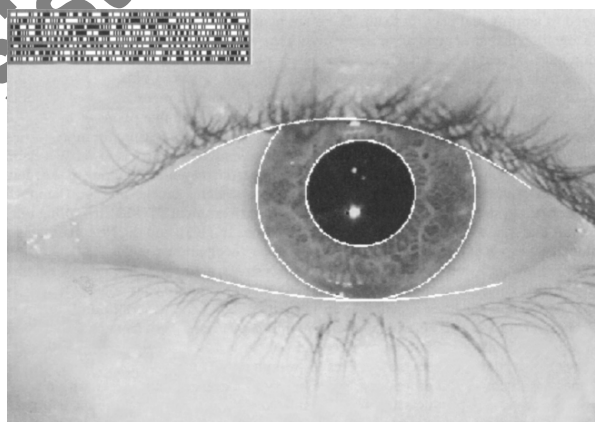
*Čitači dužice oka* analiziraju parametre dužice oka kao što su: vaskularna struktura i krvni sudovi, pegice, vlakna, korone, brazde i slično. Procedura takođe počinje identifikacijom pomoću kartice, posle koje je lice dužno da se približi i pogleda u sočivo kamere koje uzima uzorak. Dužica oka je obojeni deo oka koji okružuje zenicu, sastoji se od mreže radijalnih linija koja je jedinstvena, vremenski nepromenljiva za svaku osobu, i ne zavisi od genetskih parametara.

**Slika 27.5 Dužica oka različitih osoba**

Iako je dužica oka malih dimenzija (11 mm) i ponekad teška za slikanje, ona ima velike matematičke prednosti koje kao rezultat daju veliku razliku obrasca za pojedine osobe. Zbog činjenice da je dužica unutrašnji deo oka, ona je dobro zaštićena od okoline i stabilna tokom vremena. Relativno je neosetljiva na ugao osvetljenja i ugao gledanja, tako da specifičan okrugao oblik dužice omogućava pouzdanu i preciznu izolaciju njenih osobina i stvaranje karakterističnog prikaza. Dužica oka počinje da se formira oko trećeg meseca trudnoće, a struktura linija koje joj daju prepoznatljivost se formira se do osmog meseca, dok se formiranje pigmenta nastaviti do jedne godine posle rođenja.

Uzorak dužice oka se snima monohromatskom kamerom skrivenom iza ogledala. Osoba u ogledalu gleda odraz vlastitog oka i tako omogućuje kameri da dohvati sliku dužice. Kamera se automatski fokusira i po potrebi se uključuje dodatno svetlo. Dobijena slika se obrađuje tako da se dužica izdvaja od zenice i ostatka oka. Iz te se slike posebnim algoritmom kodiraju karakteristike i dobiva zapis koji se brzo i jednostavno upoređuje sa prethodno zapamćenim zapisom u računaru. Današnji računari mogu da uporede ogroman broj zapisa u sekundi pa je zato dužica oka izuzetno pogodna za identifikaciju. Dužicu oka je teško falsifikovati, a zbog brzog raspadanja nakon smrti upotreba tuđe dužice oka je gotovo nemoguća.





**Slika 27.6 Formiranje koda na osnovu dužice oka**

*Čitači mrežnjače oka* mere elemente koji predstavljaju obrazac rasporeda krvnih sudova u mrežnjači oka. Mrežnjača je tanko tkivo nervnih ćelija koje se nalazi se u zadnjem delu oka. Jedinstvena je za svaku osobu zbog mreže krvnih kapilara kojima je prožeta i ne menja se tokom života, osim u slučaju glaukoma i dijabetesa. Slika mrežnjače se dobija usmeravanjem laserske infracrvene svetlosti u unutrašnjost oka i podatak o položaju kapilara se dobija iz reflektovane svetlosti.

**Slika 27.7 Mrežnjača oka**

Nedostatak ovog metoda je u tome što je to delimično invazivan proces jer zahteva prodiranje infracrvene svetlosti u oko osobe nad kojom se vrši identifikacija. Zbog toga je često potrebno da upravljanjem ovim sistemom rukovodi posebno trenirani operater.

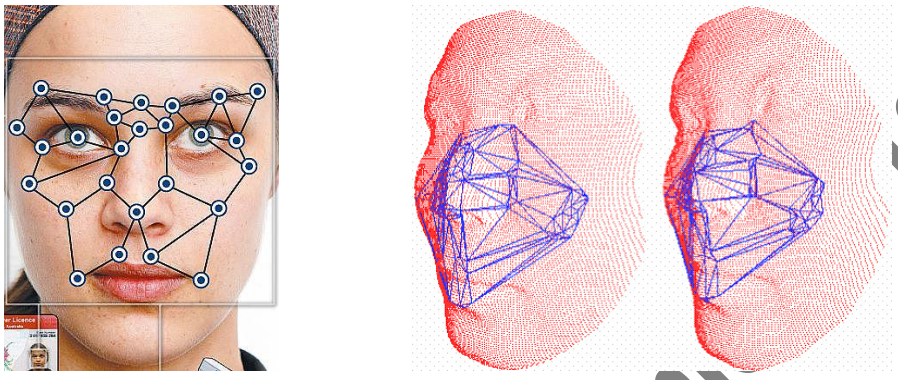
*Uređaji za prepoznavanje glasa* analiziraju zvučne parametre izgovorene fraze trajanja 1 do 1.5 s. Karakteristike ljudskog glasa potpuno su određene glasnim žicama, ustima, nosnom šupljinom i ostalim mehanizmima za stvaranje glasa u ljudskom telu. Od glasa se ne očekuje da bude potpuno pouzdana biometrijska karakteristika u smislu da omogući identifikaciju pojedinca iz velike baze podataka identiteta, ali može da koristi kao dopunski metod osnovnom metodu za identifikaciju koji se primenjuje.

**Slika 27.8 Digitalizovan uzorak glasa**

*Uređaji za prepoznavanje lica* analiziraju karakteristične linije lica (oko oka, nosa, usta, na čelu, itd.) i upoređuju sa zapamćenim podacima. Ovaj tip uređaja koji je do skoro smatran najmanje pouzdanim, razvojem tehnologije sve više ulazi u upotrebu. Danas postoje dvodimenzionalni i trodimenzionalni algoritmi kojima se realizuje ovaj biometrijski metod.

Najpoznatiji dvodimenzionalni algoritmi su *algoritmi karakterističnih lica* i *algoritmi facijalne metrike*. Algoritam karakterističnih lica upoređuje lice korisnika s unapred unesenim slikama ljudskih lica (eng. *eigenface*) – najčešće s njih 100 do 150. Za svaki *eigenface* izračunava se stepen poklapanja s korisnikovim licem, a zatim se matrica koja sadrži stepene poklapanja i koja predstavlja uzorak korisnika, memoriše na disk. Algoritam facijalne metrike analizira položaje i relativne udaljenosti između tačaka korisnikovog lica (nosa, usta i očiju) i informacije o njima se zapisuje u uzorak. Dvodimenzionalni algoritmi se lako mogu zavarati podmetanjem lažne slike. Kvalitet prepoznavanja zavisi od upadnog ugla svetlosti na lice osobe i ugla gledanja u kameru. Problem predstavlja i promenjivost lica starenjem, promena frizure, šminke, izraza lica i brade ili nošenje naočara.

Trodimenzionalni algoritmi analiziraju i memorišu 3D karakteristike i veličine delova lica. Time se izbegavaju problemi koji su karakteristični za dvodimenzionalne metode jer kvalitet trodimenzionalnog modela ne zavise od izraza lica, šminke ili ugla snimanja glave. Metodi 3D analize danas postaju konkurentni metodima koji koriste dužicu oka. Sa druge strane, algoritmi za prepoznavanje lica su brži od metoda za prepoznavanje dužice oka, i sami uređaji (kamere) jednostavniji su za rukovanje.



**Slika 27.9** Formiranje 2D i 3D uzorka za prepoznavanje lica