PRIMJENA ALARMNIH SUSTAVA U POSLOVNOM PROSTORU

Vodopija, Marta

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Marta Vodopija

PRIMJENA ALARMNIH SUSTAVA U POSLOVNOM PROSTORU

ZAVRŠNI RAD

Karlovac, 2021.

Karlovac University of Applied Sciences

Safetyand Protection Department

Professional graduate study of Safety and Protection

Marta Vodopija

APPLICATION OF ALARM SYSTEMS IN BUSINESS SPACE

FINAL PAPER

Karlovac, 2021.

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Marta Vodopija

PRIMJENA ALARMNIH SUSTAVA U POSLOVNOM PROSTORU

ZAVRŠNI RAD

Karlovac, 2021.

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
TrgJ.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Specijalistički studij: Sigurnost i zaštita

Usmjerenje: Sigurnost i zaštita

Karlovac, 07.09.2021

ZADATAK ZAVRŠNOG RADA

Student: Marta Vodopija

Matični broj: 0420418032

Naslov: Primjena alarmnih sustava u poslovnom prostoru

Opis zadatka:

1. Opisati nastanak i razvoj alarmnih sustava
2. Definirati dijelove alarmnog sustava
3. Prikazati stupnjeve tehničke zaštite i razlike stupnjevima
4. Pojasniti detektore i opisati vrste detektora
5. Analizirati dijelove sustava video nadzora
6. Pojasniti biometrijske sustave i opisati njihovu primjenu
7. Opisati sustave kontrole prolaza

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
lipanj 2021.	studeni 2021.	22. 12. 2021.

Mentor: Predsjednik Ispitnog povjerenstva:

Davor Kalem, predavač Marko Ožura, viši predavač

Zahvaljujem se svojoj obitelji, prijateljima i dečku na pruženoj potpori i strpljenju tijekom pisanja svog završnog rada i studiranja.

Iskrene zahvale i mom mentoru Davoru Kalemu, struč. spec. crim.na prijedlozima, pomoći i vođenju kroz pisanje rada.

Tema ovog završnog rada su alarmni sustavi u poslovnom prostoru. U današnje vrijeme gotovo svaki poslovni objekt upotrebljava tehničku i mehaničku zaštitu pomoću kojih se zvučno ili svjetlosno detektira neovlašten ulazak u štićeni prostor. Njihov osnovni cilj je usporavanje, detekcija i ukoliko je moguće zaustavljanje nedozvoljenog ulaska u štićeni objekt. U radu su opisani i stupnjevi zaštite kojima se štite razni objekti ovisno o stupnju ugroženosti, te razne vrste detektora i video nadzora koji doprinose jos većoj sigurnosti objekta. Ukoliko se alarmni sustavi koriste na ispravan način, rizik od nastanka štetnog događaja se svodi na najmanju razinu.

KLJUČNE RIJEČI: Alarmni sustavi, sigurnost, stupnjevi zaštite, štićeni prostor

SUMMARY:

The topic of this final paper are alarm systems in business space. Nowadays almost every office building uses technical and mechanical protection by which unauthorized entry into the protected area is detected by sound or light. Their main target is deceleration, detection and if it is possible stopping unallowed entry into the protected building. The paper also describes the levels of protection that protect various objects depending on the degree of endangerment, and various types of detectors and video surveillance that contribute to even greater security of the building. If the alarm systems are used correctly, the risk of a harmful event is reduced to a minimum.

KEYWORDS: Alarm systems, security, levels of protection, protected area

SADRŽAJ IV

ZAVRŠNI ZADATAK

PREDGOVOR

SAŽETAK

1. UVOD

Čovjek se kao pojedinac oduvijek brinuo za svoju sigurnost i sigurnost svoje imovine, te je tako još u davnoj prošlosti koristio razne signalizacije kako bi zaštitio svoj posjed od neovlaštenog pristupa. Nekada su se koristila jednostavna mehanička zvonca ili životinje koje su svojim glasanjem upozoravale na neovlašteni pristup. Takva vrsta zaštite koristila se nekoliko stoljeća, sve do 1853. godine kada je Augustin Russell Pope patentirao svoj elektromagnetni alarmni sustav, poznat kao prvi automatizirani alarmni sustav, a radio je na principu da su svi prozori i vrata bili spojeni kao nezavisne jedinice putem paralelnog strujnog kruga. Ukoliko bi se vrata ili prozor otvorili, strujni krug bi se zatvorio, što je rezultiralo vibrirajućom interakcijom kruga s pripadajućim magnetom, pri čemu su se te vibracije prenosile čekićem na zvono. Edvin Homes otkupljuje njegov patent te otvara prvu tvrtku za alarmne sustave „Holmes Electric Protection Company“. Sustavi su se postepeno razvijali sve do sedamdesetih godina prošlog stoljeća kada se u upotrebu stavljaju prvi senzori kretanja, dok su osamdesete i devedesete godine bile značajne jer su alarmni sustavi postali sve jeftiniji za ugradnju. [1]

U današnje vrijeme je gotovo nezamislivo poslovanje i zaštita bez alarmnog sustava, a on se primjenjuje i na stambenim, vojnim i industrijskim objektima, te u automobilskoj industriji, a sve u cilju sprječavanja krađa ili uništavanja imovine, te kontrole nedozvoljenog pristupa. Alarmni sustavi često se integriraju zajedno s ostalim sustavima tehničke zaštite, poput video nadzora, vatrodojave ili kontrole pristupa, čime nastaje integrirani sustav tehničke zaštite. Njihovim međusobnim djelovanjem dobivaju se dodatni podaci prilikom utvrđivanja uzroka aktivacije sustava.

2. ZAKONSKO ODREĐENJE ZA PRIMJENU SUSTAVA TEHNIČKEZAŠTITE

Prema Zakonu o privatnoj zaštiti tehnička zaštita osoba i imovine provodi se primjenom elemenata, konstrukcija, uređaja te sustava tehničke zaštite, a primjenjuje se u svrhu:

– protuprovalne, protuprepadne i protusabotažne zaštite

– zaštite od nedopuštenog pristupa u štićene prostore

– zaštite od unošenja eksplozivnih, ionizacijskih i drugih opasnih tvari

– zaštite od iznošenja odnosno otuđenja štićenih predmeta i podataka

– zaštite prilikom obavljanja poslova osiguranja i pratnje pri distribuciji novca vrijednosnih papira i dragocjenosti te drugih pošiljaka i transportu osoba.[1]

Prema Pravilniku o uvjetima i načinu provedbe tehničke zaštite, tehnička zaštita odnosi se na skup radnji kojima se na posredan ili neposredan način vrši zaštita ljudi te njihove imovine. Ova vrsta zaštite može se provoditi na razne načine, uz pomoć tehničkih sredstava, naprava ili pak sustavima tehničke zaštite, čiji je cilj, prije svega, spriječiti protupravne radnje koje su usmjerene prema štićenim osobama ili imovini kao što su:

a) Protuprovalno djelovanje

b) Protuprepadno djelovanje

c) Protusabotažno djelovanje.

Nadalje, kako bi se spriječile protupravne radnje, a ljudi i imovina bili zaštićeni, potrebno je uz pomoć raznih naprava, uređaja i sredstava postići prostornu i funkcionalnu jedinstvenu cjelinu. Također, navedeni uređaji i naprave (protuprovalna vrata, specijalne ograde i rampe, neprobojna stakla, video nadzor i sl.) bi prije svega trebale biti servisirane te održavane prema pravilima.[2]

Poslovi privatne zaštite obavljaju se unutar i oko štićenog objekta, oko štićene osobe te na javnoj i drugoj površini, unutar perimetra zaštite. Djelatnost privatne zaštite

[1]Zakon o privatnoj zaštiti (NN 16/20)
[2]Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN, 198/2003)

obuhvaća poslove zaštite osoba i imovine koji se obavljaju tjelesnom ili tehničkom zaštitom te poslove izrade prosudbi ugroženosti. Prije uspostave privatne zaštite potrebno je izraditi prosudbu ugroženosti kojom će se odrediti stvarna razina rizika od počinjenja kaznenih djela i ugrožavanja života i imovine osoba u objektu ili na javnoj površini, ovisno o vanjskim i unutarnjim faktorima ugroženosti. Pravne osobe i obrti koji su ustrojili unutarnju službu zaštite mogu obavljati poslove privatne zaštite isključivo za vlastite potrebe odnosno zaštitu osoba i imovine u objektima i prostorima koje pravna osoba koja je ustrojila unutarnju službu zaštite koristi na temelju valjane pravne osnove.[1]

Zaštita novčarskih institucija ostvaruje se korištenjem odgovarajućih prostorno-tehničkih i organizacijskih mjera te primjenom mjera tehničke i tjelesne zaštite,a sve u cilju smanjenja rizika i povećanje zaštite osoba u novčarskim institucijama.[3]

Prema Kaznenom zakonu ukoliko počinitelj učini tešku krađu obijanjem, provaljivanjem ili svladavanjem većih prepreka da dođe do predmeta iz zatvorenih zgrada, soba, blagajni ili drugih zatvorenih prostorija može ga se kazniti kaznom zatvora u trajanju od šest mjeseci do pet godina. Istu kaznu može dobiti ukoliko ukradena stvar služi u vjerske svrhe, ako je ukradeno oružje, streljivo, rakete ili akoje pri napadu imao oružje. Kaznom zatvora do deset godina kaznit će se osoba ukoliko je počinila razbojničku krađu.[4]

[3]Zakon o zaštiti novčarskih institucija (NN 56/15,46/21)
[4]Kazneni zakon (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18,126/19, 84/21)

3. ALARMNI SUSTAVI

3.1 Alarmni sigurnosni sustavi

Alarmni sustavi su temelj svake tehničke zaštite te podrazumijevaju elektroničku zaštitu objekta komponentama namijenjenima za pravovremeno otkrivanje, evidentiranje, signaliziranje i dojavljivanje korisniku zaštite o nastanku štetnih događaja na objektu štićenja. Oni su postali neizostavan dio svakog poslovnog sustava, a sve češće ih ljudi koriste i u svojim domovima jer im pružaju dodatan osjećaj sigurnosti. Zavisno o tome radi li se o unutarnjoj ili vanjskoj zaštiti, zvučnoj signalizaciji ili tihoj dojava, sustavi protuprovale se prilagođavaju potrebama korisnika sustava. Namjena sustava vanjske zaštite je prvenstveno preventivno djelovanje s obzirom da oni uočavaju sami pokušaj ulaska u prostor štićenog objekta, ponekad je dovoljno postaviti i samo lažnu kameru kako bi udaljili počinitelje. Ponekad samo aktivacija alarma i zvučna signalizacija ne budu dovoljna zaštita kako bi se zaštitio određeni stambeni ili poslovni objekt. Pravovremena reakcija i dolazak na lokaciju paljenja alarma spriječit će nastanak daljnje štete. Dojavni centri osiguravaju intervenciju zaštitarske službe na lokaciji paljenja alarma. [2]

Skoro svi objekti prikladni su za upotrebu sustava protuprovalne zaštite, a najčešće se primjenjuju za zaštitu stanova, kuća, poslovnica banaka, poštanskih ureda, mjenjačnica, benzinskih postaja, kladionica i ostalih objekata. Kako bi se iskoristio puni potencijal sustava protuprovalne zaštite potrebno je redovito održavanje sustava, pravilno korištenje istoga te kvaliteta protuprovalne opreme.

Alarmni sustavi se dijele na:

a) **žičani sustavi:** sve periferne sastavnice alarmnog sustava spojene su kabelom na protuprovalnu centralu. Centrala je kabelom spojena napajanjem 230V i telefonsku liniju
b) **bežični sustavi:**sve periferne sastavnice alarmnog sustava bežično su spojene na protuprovalnu centralu. Centrala je kabelom spojena napajanjem 230V i telefonsku liniju.Njihova upotreba je raširena u stambenim objektima te manjim poslovnim prostorima kada nije unaprijed projektirana instalacija

c) **integrirani sustavi:** povezani su naprednijim sustavom upravljanja, a pristupa im se preko mobilnih aplikacija, računala ili se mogu povezati sa nekim drugim kontrolnim ili nadzornim sustavima [3]

3.1.1 Dijelovi alarmnog sustava

Alarmni sustav se sastoji od centrale na koju se spajaju upravljačka tipkovnica, daljinski upravljači, detektori pokreta, sirene i komunikatori (GSM[5], IP[6], PSTN[7]). Ukoliko alarmni detektor pokreta zabilježi kretanje toplog tijela dok je alarm uključen, centrala će aktivirati sirenu i komunikaciju te će korisniku sustava i zaštitarskoj službi javiti na kojem se dijelu objekta odvijaštetni događaj. Nadogradnjom s videonadzorom, korisnik i zaštitari će odmahmoći vidjeti o kojem se stupnju provale radi. Detektori alarmnih sustava se dijele prema namjeni, a to su vanjski, unutarnji, žičani i bežični. [4]

Osnovni elementi alarmnog sustava su:

- protuprovalna centrala sa pričuvnim napajanjem i komunikatorom;
- tipkovnica / daljinski upravljač;
- detektori pokreta i kontakta;
- alarmna sirena sa zvučnom i svjetlosnom signalizacijom
-

Dodatne komponente detekcije stanja okoline:

- vatrodojavni detektor;
- detektor plina;
- detektor poplave / vlage

Alarmna centrala s komunikatorom: predstavlja "mozak" alarmnog sastava. Njezin zadatak je obrađivanje podataka sa svih povezanih senzora i zadavanje predprogramiranih naredbi. Neke od njih su uključivanje vanjske sirene, pozivanje korisnika putem

[5]GSM- ćelijska mreža preko koje se priključuju mobilni uređaji kako bi našli ćelije u njihovoj blizini; rade u četiri različita frekvencijska opsega.
[6]IP- adresa ili broj je specifična brojčana oznaka računala na internetu.
[7]PSTN- skup svjetskih telefonskih mreža s komutiranim krugom kojima upravljaju nacionalni, regionalni i lokalni telefonski operateri.

komunikatora namobitel te ako ste spojeni na zaštitarsku tvrtku posebnim protokolom prosljeđuje alarmnu obavijest na tzv.CDS (Centralnidojavni sustav).

Alarmne centrale vrlo često imaju ugrađeni komunikator -uređaj koji omogućuje telefonski poziv ili daljinsko upravljanje centralom te dojavu na CDS (Centralni dojavni sustav) pri zaštitarskoj agenciji.Alarmna centrala prilikom aktiviranja sustava, odnosno upisom šifre na tipkovnicu, uključujedetektore pokreta i magnete na prozorima i vratima u stanje pripravnosti detekcije. Prilikom ulaska u prostoriju, centrala će izvršiti dojavu paljenjem sirene i telefonskim / GSM / IP pozivom prema odgovornoj osobi. Odabir alarmne centrale ovisi o stupnju rizika i veličini sustava. Razlikujemo žičane i bežične (868 MHz) alarmne centrale, a u slučaju nestanka električne energije, cijeli sustav radi bez poteškoća jer ima ugrađeno vlastito baterijsko napajanje. Kod žičane alarmne centrala sve periferne sastavnice alarmnog sustava spojene su kabelom na protuprovalnu centralu, a centrala je kabelom spojena napajanjem 230V i na telefonsku liniju. Kod bežične alarmne centrale sve su periferne sastavnice alarmnog sustava bežično spojene na protuprovalnu centralu, a njihova je uporaba raširena u stambenim objektima te manjim poslovnim prostorima kada nije unaprijed projektirana instalacija.

Tipkovnica – upravljački je dio alarmnog sustava. Sadrži funkciju isključenja, uključivanja i djelomice uključenog alarmnog sustava. Tipkovnice vrlo često imaju ugrađen LCD zaslon za pregled informacija o statusu alarmnog sustava, a najčešće se upotrebljavaju u kombinaciji s kodiranim daljinskim upravljačem. Pomoću tipkovnice komuniciramo s alarmnom centralom protuprovalnog sustava. Razlikujemo žičane i bežične tipkovnice koje putem LED zaslona prikazuju status sustava, tipkovnice s ugrađenim LCD zaslonom, LCD zaslonom osjetljivim na dodir te RFID tipkovnice (aktivacija kodiranim karticama ili privjescima). Bežične tipkovnice mogu raditi na frekvenciji od 433 ili 868 MHz.

Detektori- njihov zadatak je detektirati promjene u okolini te slanje informacija u centralu. Osnovne vrste detektora koje se stavljaju unutar prostora su: detektori pokreta ili PIRdetektori, detektori vibracija i loma stakla, kontaktni detektori za vrata ili prozore, vanjski detektori kretnja.

Sirena – spaja se na centralu te zvučnim signalom oglašava alarm. Dijelimo ih na

unutarnje sirene koje su veličinom manje i manje bučne te vanjske sirene koje imaju vlastito napajanje, a zadatak im je upozoriti okolinu i provalnika da je alarm aktiviran. Sirene mogu biti žičane ili bežične. [5]

Slika 1: Shema spajanja žične alarmne centrale i elementi žičnog protuprovalnog sustava

Izvor:http://www.videonadzor.com.hr/slike/2013/alarmi/CSST/ALARMNI_SUSTAV.jpg, pristupila 05.07.2021.

3.2 Stupnjevi zaštite

Stupnjeve zaštite i ocjenu učinkovitosti sustava zaštite prvi su počeli primjenjivati predstavnici osiguravajućih društava prilikom izdavanja polica osiguranja. Na temelju procjene vrijednosti štićenog objekta ili procesa i ocjene kvalitete i učinkovitosti primijenjenih mjera tjelesne i tehničke zaštite, odobravani su popusti na police osiguranja. Predstavnici osiguravajućih tvrtki su zbog svojih potreba jednostavne klasifikacije svih štićenih objekata u nekoliko skupina bili začetnici podjele svih štićenih procesa ili procesa prema stupnjevima zaštite. Stupnjevi zaštite su povezani s vrstama primijenjene zaštite na štićenom objektu i to na način da je stupanj zaštite veći što je više primijenjenih vrsta zaštite.

Prilikom izrade koncepta zaštite pomoću definiranih stupnjeva zaštite važno je napraviti slijedeće stavke:

- procijeniti kolika je vrijednost i važnost onoga što se štiti (koliko je štićeni objekt važan i što se događa u slučaju njegova nepovratnog gubitka)

- detaljno definirati što se štiti
- procijeniti da li je vrijednost planirane uspostave sustava zaštite veća od vrijednosti samog štićenog objekta

Osnovne postavke zaštite razvrstavaju svaki objekt prema primijenjenim uređajima i opremi tehničke zaštite, ali i prema primijenjenim mjerama tjelesne zaštite. Na osnovu definiranih stupnjeva zaštite svaki objekt, proces ili osoba moraju se moći opisati jednim stupnjem zaštite što znači primjenu odgovarajućih mjera tjelesne i tehničke zaštite. Razlikujemo šest stupnjeva zaštite, a za svaki su propisane određene mjere zaštite. [6]

Prvi stupanj zaštite – najviši stupanj zaštite

Najviši stupanj zaštite koristi se za zaštitu nuklearnih centrala, važnih istraživačkih laboratorija, vojnih baza, središnjih računarskih centara, diplomatskih predstavništva i ostalih objekata od velikog značaja za državu.Ova kategorija zaštite propisuje:

- mehaničku i tehničku zaštitu kojom se detektira neovlašten ulazak u štićeni objekt i dojavljuje na CDS;
- tehničku zaštitu pomoću koje se prati kretanje u štićenom objektu i pojedinačno štićenim prostorijama (kontrola prolaza i video nadzor);
- zaštitu materijalnih vrijednosti pomoću specijalnih kasa, trezora i sl.;
- integralnu zaštitu s minimalno jednim nadzornim mjestom i sustavom veze sa zaštitarima na štićenom objektu;
- izradu sigurnosnog Plana postupanja i procedure u slučajevima mogućih incidentnih situacija.

Navedeni stupanj zaštite je cjelovit sustav zaštite i propisuje maksimalnu detekciju, usporavanje, sprječavanje i uklanjanje svakog neovlaštenog djelovanja izazvanog izvana ili iznutra štićenog objekta. To je sustav zaštite konstruiran prema načelu štićenja „u dubinu“, odnosno najzaštićenija prostorija je smještena u samom središtu objekta, a stupnjevi zaštite se formiraju od najjednostavnijeg do složenijih. Kod ove kategorije, važno je naglasiti da centralni dojavni sustav preko kojeg je objekt povezan treba imati direktnu vezu s nadležnom policijskom upravom, dok centralna nadzorna prostorija i dojavni sustav trebaju biti povezani sredstvima veze

istovremeno na više različitih načina. Cijela vanjska ograda mora biti „detektor“ nedopuštenog pokušaja ulaska u zaštićenu zonu koja će istovremeno pokrenuti alarmno stanje u centralnoj nadzorno prostoriji. Na mjestu gdje dođe do pokušaja neovlaštenog ulaza u zaštićeno područje neophodno je aktivirati svjetlosnu i zvučnu signalizaciju kako bi se čuvarima na objektu olakšalo uočavanje i brzo djelovanje. Stalna naoružana čuvarska ophodnja mora biti obučena za korištenje sredstava veze i instaliranih sustava zaštite, a njihov rad se stalno nadzire i koordiniran je iz centralne nadzorne prostorije. [6][7]

Drugi stupanj zaštite – visoki stupanj zaštite

Visoki stupanj zaštite, zbog složenosti mjera tjelesne i tehničke zaštite, koristi se za zaštitu vojnih baza manjeg značaja, bitnih industrijskih postrojenja, zatvora, rafinerija nafte i drugih objekata od bitnog značenja, gdje bi bilo kakvo ugrožavanje štićenog objekta i prostora moglo predstavljati opasnost, odnosno štetnost velikih razmjera za okolinu.

Na ovom stupnju neizostavna je:

- mehanička i tehnička zaštita kojom se detektira neovlašten ulazak u štićeni objekt,a potom se dojavljuje na Centralni dojavni sustav,
- tehnička zaštita pomoću koje se nadzire kretanje u štićenom objektu (kontrola prolaza i video nadzor),
- integralna zaštita s najmanje jednim lokalnim nadzornim mjestom i sustavom veze.

Kod visokog stupnja zaštite, glavni i prvi faktor bez kojeg se ne može uspostaviti optimalan sustav zaštite je mehanička zaštita. Vanjska ograda treba biti detektor uz obavezno korištenje zvučne i svjetlosne signalizacije kako bi zaštitari uspjeli reagirati u što kraćem vremenu. Naoružani čuvari trebaju biti povezani na minimalno dva različita načina (putem radio stanica, mobitelom, radio telefonima i slično) s centralnom nadzornom prostorijom smještenom unutar štićenog objekta, te centralnim dojavnim sustavom koji se nalazi na udaljenoj lokaciji. Ukoliko dođe do nestanka mrežnog napajanja, sigurnosna rasvjeta i pričuvno napajanje su bitni elementi jer oni trebaju omogućiti nesmetan rad nužnih elemenata sustava tehničke zaštite i potrebnu rasvjetu za rad video nadzora. [6][7]

Treći stupanj zaštite – viši stupanj zaštite

Treći, odnosno viši stupanj zaštite najčešće se upotrebljava u bankama, predstavništvima diplomata, centralama značajnih novčarskih ustanova i slično. Glavna značajka navedenog stupnja zaštite je omogućavanje unutarnje detekcije, a sve u svrhu usporavanja i sprječavanja nedopuštenog djelovanja. Upotrebljava se mehanička zaštita pomoću koje se detektira nedopušten ulaz u štićeni objekt i dojavljuje na CDS, te tehnička zaštita preko koje se bilježi kretanje unutar štićenog objekta (kontrola prolaza i video nadzor). U svrhu sprječavanja nedopuštenog ulaska bitno je koristiti veći broj obučenih i naoružanih zaštitara, a svaki od njih mora imati svoju zonu djelovanja i voditelja koji nadzire njihov rad u pojedinim zonama. Javlja se potreba za korištenjem perimetarske zaštite, koju sačinjava mehanička ograda propisane visine s mogućnošću detekcije nedopuštenog ulaska unutar zaštićenog prostora s dodatnim daljinskim nadzorom. Detekcija se obavlja elektroničkom zaštitom na samoj ogradi (detektori vibracija i sl.) i daljinski, pomoću sustava video nadzora koji omogućava daljinski nadzor, upravljanje kamerama i snimanje svih događanja te pohranjivanje video zapisa. Kako bi opisani stupanj zaštite bio što učinkovitiji neizostavna je sigurnosna rasvjeta za rad sustava video nadzora ukoliko dođe do nestanka struje te pričuvno napajanje koje omogućuje nezavisan rad nužnih elemenata sustava tehničke zaštite.[6][7]

Četvrti stupanj zaštite – srednji stupanj zaštite

Prostori koji se štite srednjim stupnjem zaštite su manje poslovnice banaka, trgovački centri, industrijski pogoni, skladišta sa većim materijalnim dobrima i slično. Upotrebljava se mehanička zaštita pomoću koje se detektira nedopušten ulazak u štićeni objekt i dojavljuje na CDS i tehnička zaštita preko koje se prati kretanje u štićenom objektu (kontrola prolaza i video nadzor) uz video zapis. Mehanička zaštita na srednjem stupnju zaštite uključuje vanjsku ogradu propisane visine, tj. minimalne visine od 2m, sigurnosnu rasvjetu, sigurnosne cilindre i ključeve, protuprovalna vrata i prozore, te druge mehaničke elemente zaštite poput metalnih grilja, barijera, rešetaka i slično. Funkciju perimetarske zaštite je moguće nadomjestiti uvođenjem sustava video nadzora s detekcijom kretanja iz video signala (video motiondetection) koja će prenijeti alarmnu informaciju do najbližeg čuvara ili u centralnu nadzornu prostoriju na štićenom objektu.

Štićeni objekt četvrtog stupnja treba imati zahtjevniji sustav tehničke zaštite koji se sastoji od protuprepadnog i protuprovalnog sustava zaštite s digitalnim prijenosom alarmne i druge tehničke informacije o vrsti, lokaciji, točnom vremenu i datumu alarmnog događaja u centralni dojavni sustav iz kojeg se neprekidno 24 sata dnevno sata prate događaji i kretanja na objektu, a u slučaju uključenja alarma pružaju se adekvatne mjere. Na samom štićenom objektu u trenutku neovlaštenog ulaska mora se uključiti zvučna i svjetlosna signalizacija i istodobno prijenos poruke u centralno nadzorno mjesto. Izuzetak od navedenog pravila je aktiviranje protuprepadnih elemenata zaštite na samom objektu koji aktiviraju tzv. „tihi alarm“, što znači da se ne uključuje zvučna i svjetlosna signalizacija, već samo prijenos alarmne poruke u centralni dojavni sustav. Na takav način se izbjegavaju situacije u kojima su osobe koje su aktivirale protuprepadnu zaštitu postale žrtve jer su najčešće svojim djelovanjem potaknule provalnike na nepredviđene poteze. [6][7]

Peti stupanj zaštite – niži stupanj zaštite

Stanovi, kuće ili skladišta s većim materijalnim vrijednostima su štićeni objekti koji se svrstavaju u niži stupanj zaštite. U pravilu se upotrebljavaju tehnička i mehanička zaštita pomoću kojih se zvučno ili svjetlosno detektira neovlašten ulazak u štićeni prostor. Osnovni cilj usporavanje, detekcija i ukoliko je moguće zaustavljanje nedozvoljenog vanjskog djelovanja koji dolazi od mogućih napadača s namjerom nezakonitog oduzimanja dobara. Ulazi, prozori i vrata štićenog objekta su glavne zone detekcije nižeg stupnja zaštite. Na tim mjestima sustav tehničke zaštite nema mogućnost prostorne detekcije, nakon mogućeg ulaska unutar zaštićenog objekta. Također ne postoji ni mogućnost prijenosa alarmne informacije u centralni dojavni sustav ili na neko drugo mjesto gdje bi se po primitku alarmne dojave mogla organizirati adekvatna intervencija, već je samo u funkciji prvotnog uzbunjivanja koji preventivno djeluje na potencijalnog napadača. [6][7]

Šesti stupanj zaštite – minimum zaštite

Objekti koji se po svojim karakteristikama i primijenjenim mjerama zaštite nalaze u ovom stupnju zaštite su najbrojniji jer predstavljaju skupinu u kojoj se nalaze prosječni stanovi i kuće koji ne posjeduju unutar štićenog objekta nikakva veća materijalna dobra. Ti objekti su zaštićeni jedino elementima mehaničke zaštite i to

klasičnim cilindarskim bravama bez upotrebe elektroničkih naprava. Zaštićeni su vratima koja nemaju dodatne točke učvršćenja te prozorima bez dodatne mehaničke zaštite. U slučaju da ipak dođe do neovlaštenog ulaska u prostor koji je šestog stupnja zaštite neće doći do nikakve aktivacije zvučne ili svjetlosne signalizacije i neće se prenijeti alarmna informacija do centralnog dojavnog sustava. Ovaj stupanj zaštite pruža minimalnu zaštitu od neovlaštenog djelovanja, sukladno činjenici da ti objekti nemaju u posjedu nikakva veća materijalna dobra. Djelovanje minimalnog stupnja zaštite može se najjednostavnije okarakterizirati kao usporavajuće u cilju sprječavanja neovlaštenog djelovanja. [6][7]

3.3 Detektori

Detektori ili alarmni senzori su elementi detekcije stanja i kretanja u prostoru. Oni su glavni dio svakog zaštitnog tehničkog sustava pomoću kojih se otkrivaju nastale promjene koje aktiviraju alarm. Mogu biti žičani i bežični na 433 ili 868 MHz frekvenciji. Detektori su izuzetno bitan faktor u zaštiti osoba te svih oblika imovine. Pravovremenim otkrivanjem topline, požara i dima mogu se spriječitiznačajne financijske štete te se smanjuje mogućnost stradavanja ljudi. [5]

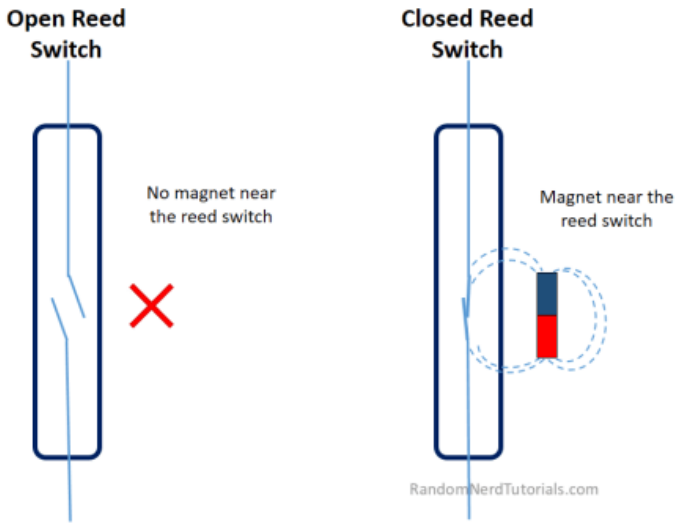
3.3.1 Vrste detektora

a) Magnetni prekidačisu vrlo jednostavni za korištenje i gotovo neprimjetni zbog svojih malih dimenzija. Lagani su i tanki, a mogu se kupiti u više različitih boja. Instalacijom magnetnog prekidača povećava se razina sigurnosti u objektu ili domu jer se može upotrebljavati i kao senzor neovlaštenog ulaska u objekt. Sastoje se od dva dijela, magneta i reed senzora[8]. Oni moraju biti blizu jedan drugome odnosno mogu biti udaljeni najviše 13mm kako bi radio ispravno. Najčešće se postavljaju na prozore i vrata,ali se mogu staviti i na ladice, kuhinjske ormariće, garažna i dvorišna vrata. Prilikom otvaranja ili zatvaranja magnetni prekidač detektira promjenu.

[8]Reed senzor ili prekidač se aktivira kada se u njegovoj blizini nalazi magnet. U sebi ima dvije male metalne žice koje se pomiču kada je u njihovoj blizini magnet i na taj se način aktivira prekidač.

Princip rada i ugradnja: kada su magnet i reed prekidač na daljini od 13 mm ili manje, reed prekidač se zatvara pod utjecajem magnetskog polja i na taj način se zatvara strujni krug. Do otvaranja strujnog kruga dolazi kada se magnet i reed prekidač počnu udaljavati. Magnetski prekidači se ugrađuju vrlo jednostavno i brzo. Nakon što se izvadi iz pakiranja, odstrani se zaštitna folija sa konektora baterije i jednostavno se zalijepi na određenu površinu sa obostranom samoljepljivom trakom. Baterija ima dug vijek trajanja zbog svoje niske potrošnje.

Koristi se za automatsku kontrolu rasvjete, kontrolu pristupa te otvaranje vrata, prozora ili garažnih vrata. Također, umanjuje rizik velike potrošnje energenata jer modul može biti opremljen temperaturnim senzorom, te posjeduje binarni ulaz za spajanje prekidača. Ugradnjom magnetnog senzora za detekciju otvaranja ili zatvaranja u objekt povećavamo pritok dodatnih informacija. Modul utvrđuje stanje otvorenosti ili zatvorenosti vrata ili prozora. Ukoliko je prozor otvoren on će zaustaviti aktiviranje grijanja ili hlađenja u željenoj prostoriji s čime se automatski rizik od visokih potrošnji svodi na minimum. Magnetni senzor možemo instalirati i na ulazna vrata kako bi otvaranjem istih automatski upalili svjetla. [8]



Slika 2: Prikaz magnetnog prekidača

Izvor:http://skr.rs/znId, pristupila 06.07.2021.

b) Detektori vibracija zidanajčešće se ugrađuju na zidove, stropove, podove, a zadaća im je otkriti vibracije podloge na koju su postavljeni. Obično imaju

potenciometar za podešavanje osjetljivosti. Detektor vibracija montira se u sredinu okvira ili zida koji se štiti, a raspon otkrivanja je preko 2m. Detektira mehaničke vibracije uzrokovane bušenjem rupa, rezanjem ili bilo kakvom drugom vrstom fizičkog oštećenja. Ugrađeni detektori pretvaraju vibracije u električke veličine pomoću svojih piezoelektričnih[9] ili mehaničkih pretvarača. Signal putuje kroz filtar koji određujepoklapa li se spektar detektiranog signala sa spektrom karakterističnim za pokušaj prolaska. Ukoliko dođe do poklapanja alarm će se uključiti.

Slika 3:Prikaz detektora vibracije zida

Izvor:https://www.alarm.com.hr/product.asp?product=visonic-detektor-vibracija-sd-304-pg2&code=00220%2DK, pristupila 06.07.2021.

c) Pasivni infracrveni detektori (PIR senzor) rade u infracrvenom spektru koje ljudska bića emitiraju u obliku topline iz tijela. Omogućavaju nam detekciju pokreta ljudskog tijela u području njegova dosega. PIR senzori su lako dostupni, jednostavni za upotrebu,mali, jeftini i imaju dug vijek trajanja. Zbog ovih značajki primjenjuju se u kućnim ili poslovnim okruženjima. Osnovni dio PIR senzora je piroelektrični element koji omogućuje detekciju infracrvenog zračenja. Senzor u detektoru je podijeljen na dva dijela koja su povezana. Rad detektora se temelji na detekciji promjene

[9]Piezoelektričnipretvarač pretvara fizičku količinu u električni napon koji se lako mjeri analognim i digitalnim mjeračem.

zaprimljenog infracrvenog zračenja na jednom od dva dijela koja čine piroelektrični element. Ako jedna od njih dobije više zračenja od druge, senzor će reagirati na tu promjenu. Zbog toga je moguće detektirati samo pokrete živih bića jer ona zrače. Uz piroelektrični element PIR senzor se sastoji i od električnog kruga koji obrađuje podatke i priprema digitalni izlazni signal od ulaznog analognog. Značajni dio korištenog PIR senzora je vrsta leće, odnosnoFresnelova leća[10] koja omogućavaraspodjelu vidljivosti na manja područja. [9]

Slika 4: Prikaz pasivnog infracrvenog detektora

Izvor:https://jablotron.com.hr/proizvod/pir-bezicni-detektor-ja-150p/, pristupila 06.07.2021.

d) Ultrazvučni detektori djeluju na način da se zvučni signal širi u prostoru i zatim se analizira reflektirani zvuk. Koriste se u „prostornoj zaštiti“ kao detektori kretanja unutar nekog štićenog prostora. Detektor prepoznaje pozadinski signal, a ako se promijeni, pretpostavlja se da je netko ušao u prostor, odnosno zasniva se na promjeni frekvencije reflektiranog zvuka od objekta koji se kreće. Sastoji se od malog zvučnika koji prenosi zvučne valove i mikrofona koji odbija reflektirane valove.Neke od prednosti su jednostavnost zadržavanja njihove energije u željenom prostoru i

[10]Fresnelova leća- zakrivljena leća velikog vidnog polja i male debljine sastavljena od niza staklenih prstenova sa zajedničkim žarištem ili fokusom. Koristi se kao sabirna leća za lokalno jače osvjetljenje ili u signalizaciji za dobivanje jačeg paralenog snopa svjetlosti.

neosjetljivost na toplinu. Ultrazvuk ne prolazi kroz zidove, a zvučni valovi se prenose na oko 40kHz što je uvelike iznad razine ljudskog sluha. [10]

e) Mikrovalni detektori Mikrovalni detektori rade na principu Dopplerovog efekta[11] te imaju predajnik i odašiljač koji rade u X (rendgenskom) području[12]. To su uređaji koji služe za detekciju pokreta po principu da zrače električno polje u određenoj zoni, a zatim mjere reflektirane signale. Ti signali se promijene kada pokretni predmet – najčešće osoba- uđe u područje detektora što uzrokuje alarm. Mogu se koristiti u otvorenim i zatvorenim prostorima. U zatvorenim prostorima mikrovalni detektori nisu previše korisni jer otkrivanje kretanja u susjednoj sobi nije potrebno. Na otvorenim prostorima se koristi za detekciju vozila u pokretu, produljenje vremena signalne grupe, najavu vozila i mjerenje brzine. Detektorima visoke frekvencije koji se koriste za najavu vozila moguće je ručnopodesiti udaljenost na kojoj se želi detektirati prijevozno sredstvo. Točkadetekcije može biti udaljena i do 100 metara od mjesta instalacije. Ovisno o usmjerenostii širini snopa detektora visoke frekvencije moguća je detekcija prijevoznogsredstva na jednoj ili više prometnih traka,a također je moguće i detektirati smjerkretanja istog. Postoje zabrinutosti oko mikrovalnog zračenja noproizvođači ističu kako je zračenje tih uređaja vrlo malo. Vrlo lako se ugrađuje i jednostavan je za održavanje, a zbog nakupljanja prašine i smoga obavezni su periodički pregledi. Svi mikrovalni detektori moraju biti u skladu s ANSI standardom IEEEC95.1 – 199913. [10]

f) Detektori dvostruke tehnologije koriste se u zahtjevnijim objektima. S njima se postiže veća pouzdanost zaštite prostora jer koriste dvostruko načelo detekcije kretanja. Dva detektora koja rade na različitom načelu detekcije nalaze se u jednom

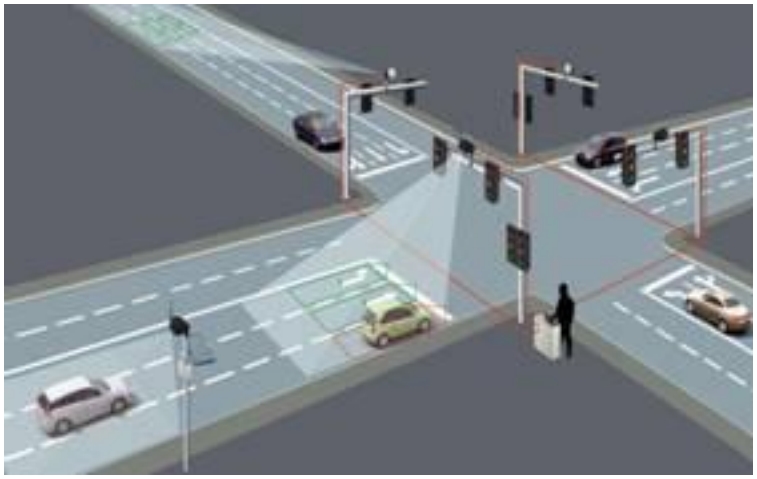
[11]Dopplerov efekt- promjena frekvencije valova pri gibanju njihovog izvora ili promatrača. Uočava se kod svakog valnog gibanja kao povećanje, odnosno smanjenje frekvencije kada se izvor valova i promatrač međusobno približavaju, odnosno udaljavaju. Koristi se u prometu gdje se uz pomoć radara određuje brzina kretanja vozila, u medicini se primjenjuje za određivanje brzine protoka krvi, a u astronomiji za mjerenje brzine radijalnog gibanja nebeskih tijela.
[12]Rendgenske zrake- odnosno x-zrake, područje su elektromagnetskog zračenja s valnim duljinama između 0,001 i 10 nm, što približno odgovara području između ultraljubičastog i gama zračenja. Koriste se u dijagnostičkoj radiografiji i kristalografiji.
[13]Standardom IEEEC95.1 – 1999- standard za sigurnosne razine s obzirom na izloženost ljudi na radiofrekvencijskim elektromagnetskim poljima 3kHz – 300GHz.Standardi su sastavljeni s nizom pravila za zaštitu kako bi se ograničila izloženost ljudi električnim poljima, magnetskim poljima i elektromagnetskim poljima.

kućištu detektora. Za alarm detektora potrebna je istovremena pobuda oba ugrađena detektora. Detekcijski element je kompletno podesiv od 180˚ sa nagibom 90˚. To pruža 10˚ do 70˚ kuta detekcije sa poljem pokrivenosti od 30 m. Visina ugradnje je do 6 metara. Najčešće se koriste za zaštitu zračnih luka, zatvora i slično.[11]

g) Video detektor

Rad video detektora zasniva se na mikroprocesorskoj tehnologiji digitalne obrade video signala. U fiksiranom kadru prometnice određuju se zone detekcije u kojima je moguće detektirati vozila u pokretu ili mirovanju uz određivanje smjera kretanja vozila. Mogu se upotrebljavati i za najavu trajanja zelenog svjetla.Kombinacijom detekcija u više različitih zona moguće je uočiti različite događaje te postoji mogućnost snimanja stanja na cesti kako bismo u slučaju nesreće mogli utvrditi uzrok i krivca. Detekcija vozila se može ostvariti u svim svjetlosnim i vremenskim uvjetima. Video detektor sadrži automatsko prilagođavanje promjenama video slike, svjetla, sjena i refleksija. Ovisno o izvedbi leće, kamere se dijele na širokokutne[14] i one s uskim kutom[15] gledanja. Na semaforski uređaj se mogu spojiti pomoću kabela ili bežično. Video detektor nalazi se u izdržljivom i laganom kućištu, vrlo lako se postavlja na željeno mjesto te se podešava pomoću prijenosnog računala. Nedostatak je izloženost vremenskim uvjetima kao što su jako sunce i magla, a prednost je vijek trajanja koji je oko 10 godina. [12]

[14]Širokokutni objektiv- ima veliko vidno polje i malu žarišnu duljinu, dok su objekti smanjene veličine, a rezolucija dobivene slike je manja. Omogućuje snimanje većih površina, pogodne su za snimanje parkirališta, ulaza u zgradu, dvorana.
[15]Objektiv s uskim kutom gledanja- približavaju i povećavaju udaljeni objekt, a vidno polje je malo. Pogodne su za snimanje uskim i manjih prostora i kada je potrebno prepoznati predmete u prostoriji.



Slika 5: Prikaz detekcije video kamere

Izvor:http://peek.hr/old/index.htm, pristupila 11.06.2021.

h) Detektor dima

Najviše korišteni detektori su optički detektori dima, a njihov zadatak je detektirati pojavudima i drugih produkata gorenja u objektu u relativno ranoj fazi razvoja požara.Omogućava detekciju širokog spektra čestica dima uglavnom generiranih požarom. U optičkim detektorima se nalaze sekcije unutar kojih se mjeri količina dima.Ako ta količina dima pređe zadanu granicu, detektor pokreće alarm. Osjetljivostdetektora se može prilagoditi uvjetima u objektu u vatrodojavnim sistemima zadojavu požara što bi značilo da se u objektima gdje su nazočni dim i prašina uuobičajenim uvjetima razina detekcije postavi na veću vrijednost, tj. neophodnaje veća doza dima kako bi se signalizirao požar, a u objektima velikog rizikapožarni alarm se aktivira odmah kod male doze dima kako bi se smanjila razinarizika. S obzirom na navedeno može se primijeniti u širokom spektru aplikacija. Na većini aplikacija su ionizacijske detektore zamijenili optički detektoriiz razloga što su precizniji u prepoznavanju sporih,tinjajućih požara. Nedostatak supoteškoće pri obavljanju poslova koji uzrokuju prljavštinu, prašinu, vodenuparu, direktna svjetlost te nisu prikladni za požare s crnim dimom i velikombrzinom strujanja zraka. Detektori se moraju zaštiti od bilo kakvog mehaničkog oštećenja te se ne smiju ugraditi bliže od jednog metra od otvora za dovod zraka. Bitno je imati stručno osoblje za periodično testiranje sustava kako bi se održao integritet svakog požarnogalarmnog sistema.

Detektori su najbitniji dio sustava za dojavu požara zatošto o brzinidetekcije ovisi reakcija na pojavu požara, odnosno štete.

Slika 6: Prikaz detektora dima

Izvor:https://pimami.hr/pametne-kuce-fibaro/sistem/senzor-dima/,pristupila 02.09.21.

3.4 Videonadzor

Videonadzor je sustav tehničke zaštite koji je nužan u svim područjima gdje se želi osigurati viša razina sigurnosti. Pruža nam osnovu za tehničku zaštitu u zaštiti ljudi i njihove imovine te minimizira zlouporabu. Dok su se u prošlosti kamere video-nazora koristile isključivo za nadgledanje, danas je prvenstveno zahvaljujući primjeni digitalne tehnologije, sustav videonadzora sastavni dio interaktivnog sustava tehničke zaštite. Videonadzor se danas najčešće koristi kao dio tehničke zaštite stambenih zgrada i malih trgovina, trgovačkih centara, hotela, banaka, bolnica, turističkih objekata, zračnih luka, poslovnih zgrada, industrijskih zgrada te raznih otvorenih prostora. Integriranjem sustava video nadzora s kontrolom pristupa, vatrodojavom i protuprovalom, perimetrijskom zaštitom i sustavima za prepoznavanje registarskih tablica, postižu se još bolji rezultati tehničke zaštite. Videonadzor se sastoji od videokamere, videonadzornog snimača te kabela. Videonadzorni snimač (DVR[16], NVR[17], CMS[18]) pohranjuje sliku s videonadzornih kamera na tvrdi disk te je

[16]DVR- digitalni video snimač; elektronički uređaj koji snima video u digitalnom formatu na diskovni pogon, USB bljesak pogon, SD memorijsku karticu, SSD ili drugi lokalni ili umreženi uređaj za masovnu pohranu podataka.
[17]NVR- mrežni video snimač; specijalizirani računalni sustav koji uključuje softverski program koji video zapis u digitalnom obliku snima na diskovni pogon, USB flash pogon, SD memorijsku karticu ili drugi uređaj za masovnu pohranu.
[18]CMS- engl. Content management system; sustav koji omogućuje upravljanje sadržajem, odnosi se na svako rješenje koje omogućuje klasifikaciju, organizaciju, povezivanje i svaki drugi oblik uređivanja sadržaja

šalje korisniku sustava. Kabel se koristi za povezivanje kamere i snimača te prenosi video signal. O kvaliteti odnosno zasićenosti bakra u kabelu ovisi kvaliteta slike s kamere. Bitna stavka svakog video nadzora je i monitor jer je svakom korisniku video sustava najvažnija visoka kvaliteta slike. Ako je kvaliteta ili rezolucija monitora loša, pokvarit će sliku i najkvalitetnije kamere ili centralnog uređaja za prikaz više kamera istovremeno kod kojeg je kvaliteta prikaza još važnija. [5]

Sustav video nadzora prvotno je korišten za nadzor događaja čije je izravno promatranje za čovjeka opasno (lansiranje raketa) ili nemoguće (ispravnost naftovoda i plinovoda) te se i danas koristi s takvom namjenom. Riječ je o specijalnim aplikacijama za nadzor npr. nuklearnih i ostalih energetskih postrojenja. Svoju širu primjenu sustavi video nadzora danas imaju prvenstveno u aplikacijama tehničke zaštite i takva njihova primjena ima najveći rast. Razvojem tehnologije videonadzor je postao jednostavniji, pouzdaniji i jeftiniji, a to su ujedno i glavni razlozi zbog čega se video nadzor sve više upotrebljava u tehničkoj zaštiti.Sustavi video nadzora imaju mnogobrojne namjene. Neke od njih su: odvraćanje od namjere štetnog djelovanja prema štićenom objektu, analiza počinjenja štetnog djelovanja unutar štićenog objekta, identifikacija osobe koja je učinila štetno djelovanje te kontrola radnih procesa. Da bi sustav zaštite ispunio svoju funkciju i bio isplativ mora se osigurati njegova pouzdanost, brzo otkloniti kvarove, osposobiti korisnike za korištenje i koristiti opremu koja tehnološki omogućava daljinsko održavanje i podešavanje. [22]

3.4.1 Vrste sigurnosnih kamera

Kamere koje su danas prisutne na tržištu se dijele prema namjeni prostora snimanja (unutarnje i vanjske), prema rezoluciji te prema osjetljivosti osvjetljenja[19]. Mogu biti nižih rezolucija (TVL)[20] ili visoke HD[21] ili FULLHD[22] rezolucije u analognoj[23], digitalnoj[24] ili IP tehnologiji[25]. Izbor kamera za video nadzor ovisi o potrebama

[19]Piksel- najmanji grafički element bitmap slike
[20]TVL- rezolucijska vrijednost; prikaz linijske gustoće koju kamera nije u mogućnosti reproducirati kao individualne linije već kao jedinstvenu sliku.
[21]HD- opisuje televizijski sustav koji pruža razlučivost slike znatno veće razlučivosti od prethodne generacije tehnologija.
[22]FULL HD- označava da je slika sastavljena od 1920 piksela vodoravno i 1080 okomito.
[23]Analogna tehnologija- podatkovni signal opisan neprekidnim funkcijama vremena
[24]Digitalna tehnologija- podatkovni signal opisan diskretnim vremenskim funkcijama

štićenog prostora i specifičnosti okoliša. Potrebno je uzeti u obzir svjetlosne uvjete, željenu razinu vidljivosti kontroliranih objekata, željenu razinu oštrine slike, željenu brzinu osvježavanja, brzinu pokretnih objekata (vozila, ljudi, materijal), kompatibilnost kamera s različitim sustavima snimanja, noćni rad, veličina, otpornost na udarce i druge posebne zahtjeve.Danas su sve više u upotrebi kamere u boji jer daju više informacija od crno-bijelih kamera. Ispravno postavljene kamere su najbolja prevencija od krađe ili oštećenja imovine, prepada, te šteta. [5]

a) **Žičane kamere:** one mogu biti teže za instaliranje, a žice mogu spriječiti pokušaje da ostanu skrivene; imaju uglavnom veću kvalitetu slike od bežičnih kamera jer njihovi signali ne putuju kroz zrak.
b) **Bežične kamere:**veća fleksibilnost, neupadljive su i prenosive, ali uređaji poput mobitela, baby monitora i bežičnog interneta mogu ometati njihov signal; negativna strana je da postoji mogućnost da se videofeed može presresti od treće strane; onene uvjetuju dodatnu instalaciju softvera, koriste web preglednike, te se mogu vrlo lako kontrolirati.
c) **Unutarnje kamere:**one imaju šire vidno polje u odnosu na standardne kamere. Mogu pokrivati skoro cijelu prostoriju jer imaju pokrivenost od 360 stupnjeva. Kamere sa fiksnim objektivom imaju mogućnost trajnog fokusiranjana neko određeno područje.
d) **Kamere sa ugrađenim detektorom pokreta:**rade na principuuključivanja detektora pokreta prije no što započne snimanje. Ovaj sistem video nadzora osigurava dodatnu razinu sigurnosti upozoravajući na sumnjive aktivnosti prije nego što dođe do njih.
e) **Podesive kamere za video nadzor:**pružaju najviši stupanj kontrole i sigurnosti. Postoji mogućnost programiranja na način da automatski preusmjere snimanje na široko vidno polje mnogo bolje nego fiksne sigurnosne kamere. Rade na daljinsko uključivanje, te imaju zoom opciju.
f) **Vanjske video kamere:**vanjski smještaj kamera video nadzora omogućuje najraniju detekciju provale, motrenjem pristupa objektu;izdržljivije su i otpornije na vremenske uvjete te imaju vodootporno kućište sa komponentama koje su dizajnirane za pokrivanje šireg prostora; prilagođene su vanjskim

[25]IP tehnologija-služi za prijenos podataka kojeg koriste izvorišna i odredišna računala za uspostavu podatkovne komunikacije preko računalne mreže.

uvjetima osvjetljenja; uspješno zamjenjuju veći broj običnih kamera u štićenom prostoru Kod vanjskih video kamera postoji mogućnosti uključivanja daljinskog snimanja, kontrole nagiba, noćnog snimanja ukoliko su opremljene infracrvenim lampicama, detekcije pokreta do bežičnog povezivanja. [13]

3.4.2 Montaža sigurnosnih kamera

Nakon određivanja područja na koje korisnik želi postaviti videonadzor, važno ga je i pravilno postaviti. Većina sustava za postavljanje videokamera je jednostavna za montažu tako da korisnik može sam instalirati opremu, ali ukoliko niste sigurni kako to izvesti na pravilan način najbolje je da to odradi profesionalac. Bitna stavka je gdje se postavlja kamera leće. Udaljenost od kamere do objekta snimanja bi trebalo pažljivo promotriti osiguravajući da je prava površina fokusirana i jasno vidljiva. Ukoliko korisnik odluči instalirati kameru na zid, bitno je osigurati da se kamera ne trese i ne iskrivljuje sliku, odnosno da je pravilno montirana. Vanjske kamere mogu pokriti velika područja, ali i spriječiti provalnike u pokušaju krađe. Moraju biti u odgovarajućem kućištu otpornom na vremenske utjecaje kako bi bila zaštićena. Čvrsta kućišta kamere mogu spriječiti vandalizam i trganje kamera. Kako bi izbjegli nepotrebno trošenje videozapisa, pojedini nadzorni sustavi imaju detektore pokreta, koji počinju snimati tek kada uređaj primijeti kretanje unutar područja snimanja. [13]

3.4.3 Prednosti i zakonske obveze

Videonadzor se sve više primjenjuje u tehničkoj zaštiti zbog velikog broja prednosti koje donosi korisnicima. Primjena videonadzora kao tehničke zaštite omogućava prepoznavanje i identifikaciju počinitelja ako dođe do počinjenja kaznenog djela. Korištenje videonadzorapostiže snažan psihološki učinak na način da potencijalnog provalnika odbija od izvršenja kaznenog djela. Također korištenje videonadzora pozitivno utječe na učinkovitost radnika te dolazi do smanjenja krađa, a procesi proizvodnje se bolje kontroliraju. Istraživanja pokazuju da se stambeni i poslovni prostori bez video nadzora puno češće nalaze na meti počinitelja kaznenih djela. Alarmi mogu pokrenuti razne događaje na kamerama kao što su: opći pokret, objekt

koji nedostaje, strani objekt, gubitak oštrine, preklapanje kamera i ispad video signala. [5]

Objekt koji je pod videonadzorom treba imati obavijest za posjetitelje kojom se naglašava da se prostor nadzire sustavom tehničke zaštite.Ta obavijest treba biti na vidnom mjestu pri ulasku u objekt i u unutrašnjosti toga objekta. Kamere trebaju biti usmjerene na onaj prostor koji se štiti. Javni prostor je dozvoljeno snimati ukoliko se radi o privatnim objektima (banke, mjenjačnice, ulazi u stambene zgrade) čije kamere zahvaćaju perimetar javne površine. Podatci prikupljeni o osobama sustavom tehničke zaštite izvan njihove zakonske namjene ne smiju biti korišteni od strane vlasnika ili korisnika objekta u kojem se nalazi videonadzor.[26]

Dužnost voditelja obrade ili izvršitelja obrade je označiti da je svaka prostorija objekta isto kao i površina izvan objekta pod videonadzorom, a ta oznaka ne smije biti dalje od ulaska u perimetar snimanja. Provođenje obrade osobnih podataka zaposlenika putem sustava videonadzora moguće jeako je poslodavac informirao zaposlenike prije donošenja odluke o postavljanju sustava videonadzora i ako su zaposlenici bili na unaprijed primjeren način obaviješteni o takvoj mjeri. Prostorije za odmor, osobnu higijenu i presvlačenje ne smije obuhvaćati videonadzor radnih prostorija.[27]

3.4.4 Oznake karakteristika kamera

- **IP zaštita** – ova oznaka označava otpornost kamere na prašinu i vlagu.

X=otpornost na prašinu; Y = otpornost na vlagu

Slika 7: Oznaka za otpornost kamere

Izvor: https://sigurnosni-sustavi.hr/kamere, pristupila 11.06.2021.

[26]Pravilnik o načinu i uvjetima obavljanja poslova privatne zaštite na javnim mjestima (NN 36/2012)
[27]Zakon o provedbi Opće uredbe o zaštiti podataka

Npr. IP54 oznaka prvom brojkom označava otpornost na prašinu, a drugom otpornost na vlagu. Što je brojka veća tim je i otpornost veća. Oznaka 5 znači da kamera ne može biti vanjska jer nije otporna na vanjski prodor prašine i vlage.Oznaka IP66 označava da kamera može biti vanjska i stajati na kiši, ali ne pod direktnim mlazom vode, dok IP67 označava da kamera može nesmetano raditi pod mlazom vode.

Slika 8: Oznaka da kamera može biti vanjska i na kiši

Izvor: https://sigurnosni-sustavi.hr/kamere, pristupila 11.06.2021.

- **IK** – označava kolika je mehanička otpornost kućišta kamere; IK40 definira kućište kamere kao „antivandal“,odnosno da kućište može izdržati silu udarca od 200N, tj. udarac od 5 kg sa 40cm visine.
- **IR ili IC** – označava ima li kamera ugrađene IR reflektore i kojeg su oni dometa (on najčešće iznosi 10 do 50m). IR reflektori su uređaji napravljeni od infracrvenih LED dioda koje po noći osvjetljuju prostor ispred kamere i omogućavaju kameri crno bijeli prikaz slike po mraku. IR reflektori su najčešće ugrađeni u kućište kamere.
- **Lux** – definira osjetljivost optičkog senzora kamere u noćnom snimanju. Oznaka 1Lux označava da kamera bez IR reflektora ne može vidjeti u mraku, dok 0,00001 Lux može vidjeti kadar po mjesečini.

LUX RATING CHART

	Condition	Light Level (LUX)	Foot Candles (FC)
Day Time	Sunlight	107,527	10,000
	Daylight	10,752.70	1,000
	Overcast Day	1,075.30	100
	Very Dark Day	107.53	10
	Twilight	10.75	1
Night Time	Deep Twilight	1.08	0.1
	Full Moon	0.108	0.01
	Quarter Moon	0.0108	0.001
	Starlight	0.0011	0.0001
	Overcast Night	0.0001	0.00001

Slika 9:Predodžba lux tablice

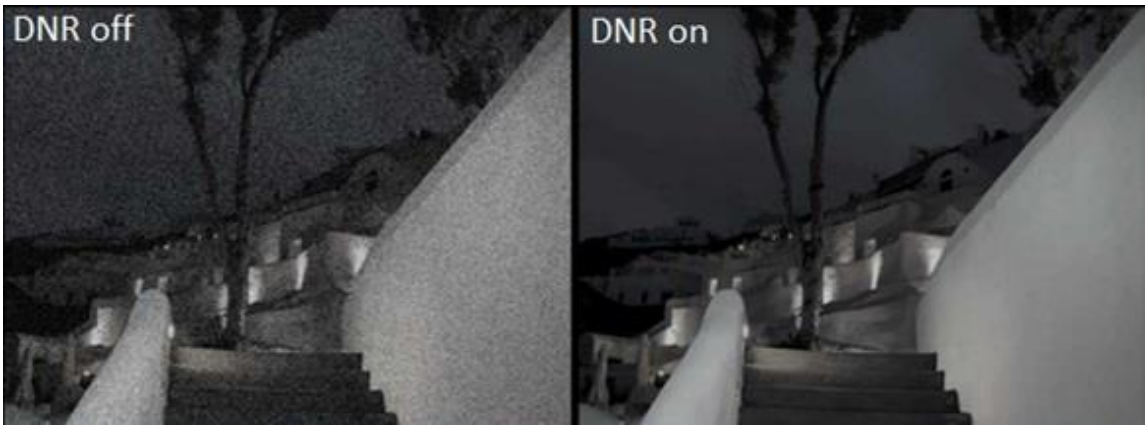
Izvor:https://sigurnosni-sustavi.hr/kamere, pristupila 11.06.2021.

- **AGC (auto gaincontrol)** – stabilizacija slike

Slika 10: Predodžba slika bez i sa stabilizacijom slike

Izvor: https://sigurnosni-sustavi.hr/kamere, pristupila 11.06.2021.

- **DNR (Digital noisereduction)** – redukcija šuma (smetnje).



Slika 11: Predodžba slike bez i sa redukcijom šuma

Izvor:https://sigurnosni-sustavi.hr/kamere, pristupila 11.06.2021.

- **BLC (backlightcompenzation)** – označava mogućnost da senzor kamere može umanjiti blještavilo pozadinskog svjetla u kadru. To znači da kada osobastoji po danjem svjetlu ispred prozora neće biti zasjenjena zbog pozadinskog svjetla i moći će se jasno vidjeti lice.

Slika 12: Predodžba slike bez i s BLC-om

Izvor:https://sigurnosni-sustavi.hr/kamere, pristupila 11.06.2021.

- **WDR (wide dinamicrange)** – definira mogućnost procesora kamere da spaja sliku duge ekspozicije sa slikom kratke ekspozicije u jednu sliku radi kompenzacije pozadinskog svjetla. Tako će npr. osoba ispred prozora biti jasno vidljiva kao i s BLC opcijom, ali će se na slici (za razliku od samo BLC-a) vidjeti jasno i kadar s prozora koji je izrazio osvjetljen. Ova opcija je izrazito

važna i propisana je kao obvezna opcija kamere za čuvanje novčarskih institucija Zakonom o zaštiti novčarskih institucija. [14]

Slika 13: Predodžba slike bez i s WDR-om

Izvor:https://sigurnosni-sustavi.hr/kamere, pristupila 11.06.2021.

3.4.5 Centralna nadzorna prostorija

Izgled centralne nadzorne prostorije

Pod pojmom centralni nadzorni sustav podrazumijeva se skup opreme, uređaja i propisanih mjera i postupaka za prijem i obradu alarmnih i drugih tehničkih informacija. Cilj je učinkovit nadzor i mogućnost brze intervencije. U izvršavanju svojih važnih zadataka centralni dojavni sustav mora ispunjavati brojne sigurnosne kriterije. Bilo koja poslovna organizacija može za vlastite potrebe izgraditi vlastiti centralni dojavni sustav. Također, postoje ovlaštene zaštitarske tvrtke sa uspostavljenim centralnim dojavnim sustavom koji pruža usluge velikom broju različitih poslovnih subjekata kojima pružaju uslugu nadzora, zaštite i povezano s time razne intervencije u cilju sprečavanja ili smanjivanja štetnih posljedica za poslovanje.

Ergonomski izvedena centralna nadzorna prostorija mora osigurati jednostavan pristup i nadzor do uređaja i opreme koji se često koriste. Razni monitori i zasloni se moraju postaviti tako da su u svakom trenutku lako vidljivi iz pozicije operatera. Visina pulta na koji se postavlja sva oprema mora biti prilagođena najnižem

operateru koji mora imati vidljivost preko pulta do najudaljenijih monitora. Na pultu mora biti predviđen dovoljno veliki horizontalni prostor za postavljanje knjige evidencije, tipkovnica, telefona, radio stanica i slično, a radna površina mora biti nereflektirajuća. Uređaje i opremu koji se nalaze u centralnoj nadzornoj prostoriji potrebno je periodično testirati i ispitivati njezinu funkcionalnost. Svako izvršeno testiranje mora biti evidentirano zajedno s rezultatima. Pravilno projektiran centralni dojavni sustav mora biti zaštićen protuprovalnim i protuprepadnim sustavima, sustavom kontrole pristupa, video nadzora i odgovarajućim mjerama tjelesne zaštite. Najvažniji faktor i pokazatelj učinkovitosti i kvalitete centralnog dojavnog sustava je školovani operater. O njegovim vještinama, odnosno znanju, uvježbanosti i pravovremenoj reakciji ovisi uspješnost svih ostalih elemenata u propisanim procedurama i reakcijama nakon prijema poruke. [6][15]

Slika 14: Nadzorna prostorija

Izvor:https://poslovnasigurnost.hr/wp-content/uploads/2019/03/First-Alarm-LLC.jpg, pristupila 11.06.2021.

Smještaj centralnog dojavnog sustava (CDS) i zahtjevi na građevinu

Za svaku prostoriju u odabranoj građevini nužno je znati svrhu, broj i vrstu redovnih i privremenih korisnika. U zgradi u kojoj se nalazi centralni dojavni sustav potrebno je imati vatrodojavni sustav. Preporuka je da centralna nadzorna prostorija ima izlaz ili vrata u slučaju opasnosti, a u prostoriji bi sva vrata morala imati propisani nivo

vatrootpornosti. Prostorija mora biti klimatizirana te u zgradi mora postojati vatrodojavni sustav. Nakon pronalaska prihvatljive lokacije i ispunjenja kriterija koji su predodređeni za objekt, postavlja se oprema i elektronički uređaji koji se spajaju na uređaje za napajanje s primjerenom naponskom zaštitom. U slučaju da dođe do nestanka struje i prebacivanja na pomoćno napajanje, u centralnoj nadzornoj prostoriji i pridruženim prostorima nužno je predvidjeti rasvjetu sa što kraćim vremenskim uključenjem i prebacivanjem na pomoćno napajanje.

Zahtjevi za operatere u centralnom nadzornom prostoru

Za vrijeme konstruiranja centralnog dojavnog sustava nužno je ustanoviti koliki će biti broj skupljenih poruka i korisnika koji imaju ugrađene sustave zaštite. Pomoću tih analiza izgrađuje se simulacija najvećeg opterećenja vezanih za prijem i obradu alarmnih i drugih tehničkih poruka. Poruke se sakupljaju i analiziraju 24 sata dnevno, a zaprimaju ih i analiziraju operateri i upravo zbog toga je bitno definirati njihov broj i zadatke u pojedinoj smjeni. Centralni dojavni sustav mora imati voditelja, odnosno odgovornu osobu i potrebno je da postoji uvijek osoba u pripravnosti koju voditelj u slučaju potrebe može rasporediti. Bitan faktor prilikom ocjenjivanja kvalitete CDS-a predstavlja očekivano vrijeme reakcije tehničkog osoblja u slučaju kvara ili pogreške uređaja i opreme koji se nalaze u centralnoj nadzornoj prostoriji, ali isto tako i vrijeme uklanjanja kvara i vraćanje u ispravno stanje. Zbog tih razloga neophodno je redovito izvoditi simulacije kvara i na temelju toga provoditi testiranja i neprestanu edukaciju zaposlenika. Svi zaposlenici koji imaju odobrenje ulaska u zaštićeni prostor centralne nadzorne prostorije moraju imati identifikacijsku iskaznicu pomoću koje se registriraju i omogućava im se prolaz na električnom sustavu kontrole pristupa. [6][15]

3.5 Biometrijske brave

Riječ biometrija dolazi od starogrčkih riječi bios = „život“ i metron = „mjera“.Biometrija je znanost o postupcima za jedinstveno prepoznavanje ljudi, na temelju uspoređivanja jednog ili više urođenih tjelesnih obilježja. Bavi se identifikacijom pojedinaca, temeljenoj na njihovim biološkim karakteristikama ili karakteristikama ponašanja. Vrlo često se koristi u područjima medicinske dijagnostike, informatičke sigurnosti,privatne zaštite, nadzora kretanja na određenim javnim prostorima (autentifikacija), identifikacije osoba za nekriminalističke potrebe, poput nadzora

izbora, dokazivanja očinstva i dr. Biometrijska tehnologija koristi jedinstvena obilježja bioloških karakteristika ljudskog bića, odnosno obilježja nositelja koje nisu otuđive i nije ih moguće jednostavno kopirati. [6]

Svaka osoba, životinja ili predmet je specifičan i identičanisključivo sam sa sobom, odnosno razlikuje se od svih drugih. Uvjeti po kojima je različit od ostalih su individualna obilježja, a jedan dio tih obilježja, koja se mogu koristiti u postupku identifikacije nazivaju se identifikacijska obilježja. Kako bi se određeno obilježje moglo upotrijebiti u postupku identifikacije treba zadovoljiti pojedine kriterije. Neki od njih su:

- jedinstvenost (mora ga imati svaka osoba)
- individualnost (mora se razlikovati kod svakog čovjeka)
- trajnost i nepromjenjivost
- mogućnost izdvajanja iz ukupnosti obilježja (zbog mogućih kreiranja baza)
- jednostavno prikupljanje i korištenje. [16]

3.5.1 Princip rada biometrijskih brava

Biometrija se koristi kod jednostavnijih zaštita kao npr. zaštita mobilnog uređaja, tableta preko otiska prsta, dok su biometrijske brave odlična zaštita s obzirom da su biometrijske karakteristike jedinstvene i neotuđive. Izvrsna su zaštita od krađe te ne postoji rizik od gubitka ključeva, kartica, privjesaka te slično. Otvaraju se vrlo brzo, neke i za manje od jedne sekunde. U pojedinim modelima biometrijskih brava postoji mogućnost pregleda povijesti ulaska i izlaska korisnika odnosno zaposlenika. Na taj način sprječava se zloupotreba i posuđivanje kartice kod evidencije radnog vremena. Mogu se postaviti u kuću, stan ili poslovni objekt. Nema straha da ćete izgubiti ili zaboraviti lozinku. Ukoliko dođe do nestanka struje, brave su instalirane sa alternativnim sistemom otvaranja vrata koji zahtijeva mehanički ključ, digitalni kod ili pristup kartici. Nema rizika da neovlaštena osoba uđe u zaštićenu prostoriju upotrebom tuđe kartice. Biometrijske brave dozvoljavaju isključivo ovlaštenim osobama ulazak u prostoriju, kuću ili stan. Postoje dva modela biometrijskih brava, beskontaktne i na dodir. Beskontaktne biometrijske brave rade na principu

prepoznavanja oka,glasa ili crta lica, dok biometrijske brave na dodir koriste isključivo otiske prstiju za ulazak u prostoriju. U slučaju ako je osoba prepoznata od strane kompjuterskog sistema dozvoljen joj je ulazak, vrata se otvaraju. [17]

Za biometrijske sustave identifikacije kao najznačajnije tehnologije primjenjuju se:

3.5.1.1 Identifikacija otiska prsta

Otisak prsta se smatra najstarijom i najpoznatijom metodomautentifikacije. Autentifikacija je proces utvrđivanja identiteta određenog subjekta, npr. upisivanje PIN-a kod korištenja bankomata, upisivanje korisničkih podataka i lozinke i slično. Subjekt treba dati određene podatke po kojima druga strana može utvrditi da je subjekt upravo taj kojim se predstavlja.

Metodom analize pojedinosti analiziraju se relativni položaji jedinstvenih karakteristika otiska prsta kao npr.: završeci grebena (predstavlja točku u kojoj se greben naglo završava), bifurkacije (mjesto na kojem se dvije linije spajaju u jednu), uzorak izbočina i udubljenja na površini jagodice prsta. Otisci prstiju su različiti kod svakog čovjeka, čak i kod jednojajčanih blizanaca. Otisak prstaje metoda koja je lako dostupna te se najčešće koristi zbog jednostavnosti. Postoje tri tehnike za skeniranje otisaka prstiju: optički čitač, silicijski čitač i ultrazvučni čitač. Optički čitač je način zapisa podataka gdje se čitanje ili pisanje izvodikorištenjem svjetla i optičkih pojava te ti podatci odlaze na optički disk.Silicijski čitač spada u silicijski sustav koji je pripadao američkoj poluvodičkojtvrtki koja je imala sjedište u Tustinu u Kaliforniji.[18]

Slika 15: Identifikacija otiska prsta

Izvor:https://www.pni.hr/media/catalog/product/cache/f8a70b59eb59601202eca23a448e83c1/P/N/PNIFT05_1.jpg, pristupila 03.09.2021.

Slika 16: Identifikacija otiska prsta

Izvor: http://skr.rs/znIJ, pristupila 03.09.2021.

3.5.1.2 Identifikacija otiska dlana i prstiju

Metoda identifikacije dlana provodi se snimanjem ruku (debljina, širina, površina), te automatskom usporedbom obilježja poput rasporeda, oblika i duljine kostiju. Postoji oko 90 obilježja koja se temelje na navedenim diferencijalnim karakteristikama.
S obzirom na to da geometrija ruke nema zadovoljavajuću razinu jedinstvenosti kod svakog čovjek, odnosno radi se o prilično nepreciznoj metodi, ona se uglavnom koristi u procedurama provjere identiteta,tj.autentifikacije. U postupku identifikacije može se koristiti kao kombinacija sa drugim metodama kao prvotna metoda. Jedna od novijih metoda identifikacije na temelju dlana i prstiju, temeljene na modernim tehnologijama je i metoda usporedbe rasporeda vena na šaci, tijekom koje se pronalaze mjesta gdje se spajaju krvne žile koje sačinjavaju specifičnu šaru. Navedena metoda pripada skupini bezbolnih metoda, te se koristi u objektima gdje je potrebno u vrlo kratkom vremenu usporediti veći broj uzoraka, bez velike pouzdanosti. [16][18]

Slika 17: Identifikacija otiska dlana

Izvor:https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQ-n7SmLbZtDttt3q1UZdjpuFlx9rA-4ao-q5DJ2NrFybeN-fkKECi9tQhC3lN18Z8t3l4&usqp=CAU, pristupila 03.09.2021.

3.5.1.3 Identifikacija karakterističnih crta lica

Prepoznavanje lica je najprirodniji način prepoznavanja među ljudima. Na licu je moguće mjeriti i uspoređivati čak preko 80 obilježja koja se ne mijenjaju tijekom vremena, kao što su npr. razmak očiju, širina nosa, dubina očnih udubljenja, jagodice, vilica, brada itd. Nabrojane značajke se mjere (otprilike njih 20-ak), te se oblikuje numerički digitalni kod koji prikazuje lice u bazi podataka. Zadržavanje od prosječno par sekundi u vidnom polju kamere bit će dovoljno da sustav identificira osobu i provjeri s pohranjenim podacima u svojoj bazi radi usporedbe. Kada se točno i pouzdano želi odrediti identitet osobe koja se našla u promatranom području onda je sustav uvijek dodatno pojačan ljudskim faktorom. U praksi na usmjeravanim prolazima se postavlja video kamera koja pohranjuje sve fotografije prilikom prolaska ljudi i te podatke pohranjuje u bazu. Nakon usporedbe s ostalim „označenim“ podacima iz baze donosi se odluka od zaustavljanju takve osobe.

Razlikujemo dvodimenzionalne i trodimenzionalne algoritme za prepoznavanje lica.Kod korištenjadvodimenzionalnih algoritama za usporedbu lica, najpoznatije metode su algoritam svojstvenihlica i algoritam facijalne metrike. Algoritam svojstvenih lica je metoda u kojoj se lice osobe uspoređuje s unaprijed unesenim i pohranjenim slikama ljudskih lica, a algoritam facijalne metrike je metoda kojom se

analizira položaj i relativna udaljenost izmeđudijelova korisnikova lica (nosa, usta i očiju).Dvodimenzionalni algoritmi se lako mogu zavarati podmetanjem slikelegitimnog korisnika. Kut pod kojim je izvršeno snimanje lica i kut upada svjetlosti na lice osobe bitni su kod kvalitete prepoznavanja. Nedostatak kod dvodimenzionalnog algoritma je promjena frizure, promjenjivost lica starenjem, način šminkanja, nošenjem naočala ili brade. Zbog nepouzdanosti i nepreciznosti dvodimenzionalni algoritmi se ne koriste često u identifikaciji.

Slika 18: Identifikacija lica

Izvor:https://novo.hr/wp-content/uploads/2020/01/prepoznavanje-lica-biometrija.jpeg, pristupila 04.09.2021.

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.

Prepoznavanje lica koristi se tragajući za nestalim osobama, a široka uporabaprimjećuje se i kada je riječ o sigurnosti, npr. može se zabraniti ili dopustiti pristup određenim osobama ovisno o tome kako sustav identifikacije reagira na lice osobe. Mogu se koristiti i u potvrđivanju identiteta osoba kod odlazaka na izbore. Osim toga, implementiraju se rješenja koja bi se moglaiskoristiti u obrazovnim ustanovama radi autentične i jednostavnije provjere dolaska studenata na predavanja, te kod pristupanja ispitima kao potvrda da studenti koji polažu ispite

doista i jesu te osobe. Na društvenim mrežama između ostalog postoji instalirana mogućnost raspoznavanja lica osoba i predlaganja istih za označivanje na fotografijama koje se postavljaju. Na kraju, bitno je napomenuti analiziranje video snimki u cilju raspoznavanja ljudi gdje računala mogu raspoznati otprilike 100 ljudi u vremenskom razdoblju u 5-6 sekundi, dok bi za usporedbu čovjeku trebao i čitav dan.[16][18]

3.5.1.4 Identifikacija zjenice oka

Identifikacija na temelju zjenice oka je jedna od pouzdanijih metoda jer se koristi u strože kontroliranim uvjetima i u manjim sredinama gdje postoji veća disciplina prilikom očitanja. Ljudsko oko sadrži iznimno veliki broj individualnih karakteristika koje ga čine izuzetno povoljnim za postupak identifikacije osoba. Posebno pogodnim za identifikaciju pokazali su se šarenica i mrežnica oka.

Mrežnica je tanka kružna stanica isprepletena krvnim žilama, a smještena je u stražnjem dijelu oka. Njezina građa je individualna i specifična značajka pojedine osobe upravo zbog krvnih kapilara kojima je ispunjena. Smatra se da je ovo jedna od sigurnijih biometrijskih značajki jer se mrežnica ne mijenja za vrijeme života niti je moguće promijeniti odnosno kopirati unutrašnju građu oka. Kako bi se uspješno skenirala mrežnica oka nužno je maknuti naočale, približiti oko skeneru, te centrirati pogled na odgovarajuću točku. Postupak skeniranja je vrlo kratak i traje otprilike 10 do 15 sekundi. Oko se tijekom procesa skeniranja obasjava snopom svjetlosti, odnosno laserska infracrvena svjetlost se usmjerava u oko, a reflektirana svjetlost nam daje informacije o položaju kapilara. Ovakva metoda svrstava se u neugodnije metode, a zbog vrlo visoke pouzdanosti primjenjuje se u područjima visokog stupnja sigurnosti.

Šarenica ili iris obojeni je dio oka koji okružuje zjenicu, a sastoji se od prstena, brazdi ipjega u raznim bojama, koji čine jedinstven kompleks boja i šara kodsvakog čovjeka.Ona je jedinstvena i trajna i ne postoji mogućnost mijenjanja njezine strukture bez rizika od sljepoće, te je upravo zbog toga izuzetno praktična za identifikaciju. Sustav nije moguće prevariti nošenjem leća jer postoje računalni programi koji ih registriraju.Nije moguće prevariti sustav ni staklenim ili pravim okom

odstranjenim s mrtvog čovjeka jer odvajanjem od tijela organ gubi svoje karakteristike i ne dolazi do širenja zjenice prilikom obasjavanja oka. Ovakva metoda identifikacije je jednostavna, pouzdana zbog prirodnih značajki šarenice i neinvazivna jer ne dolazi do fizičkog kontakta sa skenerom.[16][18]

Slika 19: Identifikacija zjenice oka

Izvor:https://www.racunalo.com/wp-content/uploads/2016/07/Biometrijska-identifikacija-sve-je-%C4%8De%C5%A1%C4%87i-oblik-sigurnog-pla%C4%87anja-01-630x355.jpg, pristupila 04.09.2021.

3.5.1.5 Identifikacija glasa

Glas je individualno obilježje osobe koje je vrlo jednostavno registrirati i utvrditi istovjetnost glasa ljudskim sluhom. Identifikacijom govornika se bave stručnjaci koji imaju primarno akademsko obrazovanje u području lingvistike, fonetike, patologije glasa i govora i/ili akustike te stručno znanje i iskustvo u forenzičnoj analizi jezika, glasa i govora. Prepoznavanje glasa koristi se za identifikaciju korisnika na temelju njegovih jedinstvenih glasovnih karakteristika glasa poput boje glasa, frekvencije, modulacije, govornim manama, specifičnostima izgovora određenih glasova i slično. Osoba mora izgovoriti neki tekst koji je prethodno izgovorio i koji je spremljen u bazu podataka kako bi se identificirao. Audioforenzičari kombiniraju slušnu i spektografijsku metodu za identifikaciju glasa pri čemu koriste različita akustička mjerenja te uspoređuju rezultate kako bi se povećala točnost identifikacije. Tako se raspoznavanje glasa definira kao kombinacija zvučne i spektografijske usporedbe jednog ili više poznatih glasova s nepoznatim glasom u svrhu identifikacije ili eliminacije. Prednost sustava za identifikaciju je korištenje uobičajene, jeftine i lako

nabavljive hardverske opreme, a nedostatci su velika mogućnost zavaravanja sustava, sustav je osjetljiv na pozadinsku buku i variranje glasa ovisno o dobi i raspoloženju osobe. [16][18]

3.6 Sustav kontrole pristupa

Jedan od najvažnijih elemenata sustava tehničke zaštite je kontrola pristupa.U početku se sustav kontrole prolaza koristio većinom u visoko sigurnosnim sustavima, ali zbog sve pristupačnije cijene te usavršavanja omogućeno je koristiti sustav kontrole pristupa u svakodnevnom životu.

Cilj kontrole pristupa i prolaza je zaštititi poslovni ili stambeni objekt od neovlaštenog ulaza, nadzirati ulazak i izlazak te na taj način povećati razinu sigurnosti. Kontrolom prolaza se također nadzire iznošenje ili unošenje nedozvoljenih materijala iz ili u prostor. Može se koristiti za zaštitu cjelokupnog objekta ili za zaštitu posebno štićenih cjelina kao npr. ured direktora, ulaz u stambenu zgradu, server sobe, arhivske prostorije, upravljačko-nadzorne sobe, parkirališta, dizala, skladišta i trezora. Također, koristi se i za dokazivanje identiteta za ulazak u zaštićene prostore, automobile, pristup računalima ili zaštićenim podacima. U kombinaciji sa sustavima kontrole pristupa koriste se i sustavi video nadzora, digitalno snimanje i pohranjivanje podataka kako bi se sigurnost podigla na veću razinu.

Pravilno projektirani, izvedeni i održavani sustavi kontrole pristupa i evidencije radnog vremena daju najviše informacija o kretanju unutar štićenog prostora, radnim navikama i disciplini zaposlenika, uz relativno mala financijska izdvajanja u odnosu na ostale sustave tehničke zaštite. Prethodno opisani čimbenici bitno utječu na podizanje stupnja sigurnosti svih osoba koje se stalno ili povremeno nalaze unutar štićenog prostora, što je i zadaća sustava zaštite. [18]

Zajednička je karakteristika sustava kontrole pristupa da se sve prikupljene informacije o ovlaštenim i neovlaštenim pokušajima ulaska u zaštićeni prostor registriraju, pa se iz toga nameće logičan zaključak o mogućnostima korištenja prikupljenih informacija i svim prolascima za evidentiranje radnog vremena zaposlenika unutar poslovnog objekta neke tvrtke i to prilikom prve i posljednje registracije tijekom jednog dana bez obzira na lokaciju registracije.

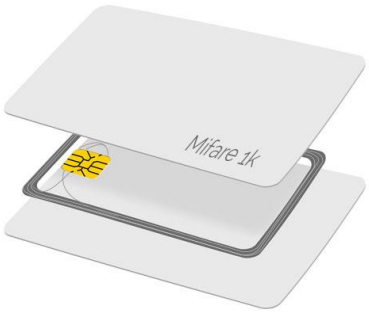
Najčešći podaci koji se ispisuju na prednjoj strani kartice su:

- ime i prezime korisnika,
- fotografija,
- oznaku (logo) tvrtke,
- jedinstveni broj nositelja kartice
- oznaku ili naziv poslovne jedinice kojoj nositelj kartice pripada. [18]

Kako bi se identificirali korisnici najčešće se koriste RFID[28](Radio-frequencyidentification) beskontaktne kartice koje imaju ugrađeni čip za kontrolu prolaza. Osim RFID kartica koriste se i RFID naljepnice, narukvice, privjesci i dualne kartice.

RFID karticesu veličine kao i uobičajene bankovne kartice, tj. 86 x 54. Ako se radi o prometnom i zahtjevnom mjestu korištenja kao što su lokacije na kojima prolazi puno osoba, mjesta na kojima je potrebna brza identifikacija, preporuča se 125 kHz tehnologiju koja se često naziva i proximit[29]. Ako se radi o mjestima na kojima nema velikog prometa, a kartice će djelovati na blizinu, preporuča se 13,56 tehnolgiju ili *Mifare*[30], kao i *NFC*[31]. NFC se dosta često koristi i vrlo je popularan u posljednje vrijeme osobito pri identifikaciji u financijskom sektoru. Često se ovakve kartice koriste kada zaposlenici koriste određene usluge u organizacijama, npr. prilikom korištenja kopirnih aparata, kod plaćanja obroka ili kava, kod korištenja teretane. [19]

[28]RFID u prijevodu s engleskog znači identifikacija radio frekvencije
[29]Proximity card- odnosno približna kartica je beskontaktna pametna kartica koja se može čitati bez umetanja u uređaj čitača
[30]Mifare- zaštitni znak u vlasništvu NXP semiconductors serije čipova integriranog kruga koji se koriste na frekvenciji 13,56 MHz
[31]NFC- engl. Near field communication, bežična tehnologija koja radi na malim udaljenostima od samo nekoliko cm



Slika 20:RFID kartica

Izvor:https://1klik.com.hr/wp-content/uploads/2015/07/programiranje-kartica.jpg, pristupila 16.12.2020.

RFID naljepniceConfidex UHF naljepnica za prednje staklo automobila posebno je osmišljena za kvalitetnu i brzu identifikaciju vozila. RFID oznaka UHF-a dizajnirana je za vjetrobransko staklo vozila i prikladna je zavelik izbor automatskih aplikacija za provjeru vozila, kao što su kontrola pristupa, parkirna dozvola, naplata cestarine ili potvrda o osiguranju. Proizvod se ne može prenositi niti posuđivati jer se ne može eliminirati sa stakla bez uništavanja.[19]

Slika 21: RFID naljepice

Izvor:https://1klik.com.hr/wp-content/uploads/2015/01/RFID-naljepnice-225x225.jpg, pristupila 16.12.2020.

RFID narukvice FID narukvice služe za beskontaktnu identifikaciju, a pogodne su za ugostiteljske i hotelske objekte u kojima se zahtijeva higijenski pristupačna i

jednostavna provjera gostiju i zaposlenika. Narukvice mogu raditi na frekvencijama od 125 kHz i 13,56 MHz, a doseg na kojem prepoznaje broj iz narukvice je između 8 i 10 centimetara udaljenosti od RFID čitača. Narukvice su elastične, vrlo dobro prianjaju uz ruku osobe koja ju nosi, te su 100% vodootporne. Također, otporne su na vanjske utjecaje i nemaju rubove, kopče i slično.[19]

Slika 22: RFID narukvice

Izvor:https://1klik.com.hr/wp-content/uploads/2015/01/28515506_m1-100x100.jpg, pristupila 16.12.2020.

RFID privjesciprikladni su za upotrebu na sportskim terenima te u svrhu identifikacije pri ulasku i izlasku iz štićenih objekata. Praktični su jer se mogu koristiti kao privjesak za ključeve te su malih dimenzija i stanu u džep. Mogu biti različitih boja te različitih frekvencijskih izvedbi.[19]

Slika 23:RFID privjesci

Izvor:https://1klik.com.hr/wp-content/uploads/2015/01/rfid-privjesci-100x100.jpg, pristupila 16.12.2020.

Dualne (hibridne) kartice su kartice s dvije frekvencije, koje imaju dvije pločice koje funkcioniraju na različitim frekvencijama, odnosno 125 kHz i 13,56 MHz. One se koriste ukoliko je potrebno potvrditi identitet osobe prilikom ulaska u poslovan objekt, a zatim i u ured. S obzirom da čitač na ulazu u zgradu i ured ne rade na istoj frekvenciji potrebne su dvije frekvencije. Dualna kartica omogućuje korisniku da lako koristi jednu karticu s više čitača, koji ne rade na istoj frekvenciji. [19]

Prednosti:

1. Primjenom kontrole pristupa i prolaza u poslovnim objektima umanjuju se sigurnosni problemi ukoliko dođe do gubitka ili krađe kartice u odnosu na slučaj kada se upotrebljava klasični ključ. Svaki korisnik ima jedinstvenu karticu ili identifikacijski element, ako se radi o biometriji, što daje mogućnost za individualnu kontrolu i praćenje aktivnosti.
2. U slučaju kada zaposlenik trajno napušta poduzeće nije potrebno provoditi sigurnosne mjere kao što su promjene brava i sl., već se samo poništava njegova identifikacijska kartica.
3. Sustav kontrole pristupa daje svakoj osobi pristup u različita područja sukladno programiranim pravilima, a svaki neovlašteni pokušaj ulaska ostaje zabilježen. Ovaj sustav je vrlo prilagodljiv, a promjene su jednostavne i brze. [2]

Digitalna brava –Yale GATEMAN

Sustavi za zaključavanje Yale[32] idealni su za sve vrste poslovnih, rezidencijalnih, apartmanskih i ostalih prostora visokih sigurnosnih zahtjeva. Također koriste se i u hotelima, na parkiralištima te dizalima.

Digitalna bravaYale GATEMAN YDM3109

Ovaj proizvod je osmišljen i proizveden tako da osigura osobnu sigurnost. Yale GATEMAN je precizan elektronički uređaj, ali ukoliko se nepravilno koristi može dovesti do oštećenja ili gubitka imovine. Prije početka rada s uređajem potrebno je

[32]Yale- jedna od najstarijih svjetskih marki i vjerojatno najpoznatije ime u području rješenja za zaključavanje, a dio je grupacije ASSA ABLOY u kojoj se nalazi i poznati brand Multi-T-Lock

proučiti sve sigurnosne upute i upute o načinu korištenja. Prije ugradnje potrebno je provjeriti sa prodavačem postoji li mogućnost ugradnje uređaja na tip vrata koji kupac posjeduje jer se standard koji uređaj koristi može razlikovati od onoga koji kupac ima.

a) Karakteristike

- uz RFID kartice koje se isporučuju s uređajem moguće je koristiti sve kartice tipa ISO 1443A[33]
- u slučaju gubitka RF kartice ponovnom registracijom preostalih kartice poništava se izgubljena.
- konkretno, ovaj model uređaja podržava maksimalno 40 RF-kartica.
- istovremeno doticanje uređaja s većim brojem kartica koje u sebi imaju RFID čip neće dovesti do blokade uređaja. Bez obzira na broj kartica uređaj će detektirati samo onu koja je ranije programirana.
- svjetlosni i zvučni indikatori upozoravaju na stanje baterije. U slučaju kada su baterije u potpunosti ispražnjene, moguće je upotrijebiti standardnu 9V bateriju kako bi se omogućilo korištenje uređaja.
- uređaj se može prema potrebi stišati ili se zvučna upozorenja mogu u potpunosti isključiti.
- moguća je ugradnja daljinskog modula koji podržava 5 daljinskih upravljača. Bežična „FloatingID“[34] tehnologija garantira sigurnost i omogućuje rad s udaljenosti do 50m.

[33]ISO 1443- beskontaktne kartice s integriranim krugom, međunarodni standard koji definira blizinu kartice koje se koriste za identifikaciju

[34]„FloatingID“- tehnologija kojom uređaj koji ima ugrađen čip svaki puta pošalje različitu informaciju kako bi se povećala sigurnost uređaja

Slika 24: Prikaz digitalne brave Yale GATEMAN YDM 3109

Izvor:http://www.es-s.hr/index.php/hr/digitalne-brave, pristupila 16.12.2020.

b) Načini pristupa

Brava Yale GATEMAN ima tri načina pristupa: PIN-kod, RF-karticu i klasičan mehanički ključ. Registracija RF kartica: u slučaju gubitka jedne ili više registriranih RF kartica potrebno je ponovo registrirati preostale kartice čime se izgubljene kartice poništavaju i postaju bezvrijedne. U slučaju pronalaska izgubljene kartice izvršite ponovnu registraciju svih kartica koje posjedujete.

Registracija PIN-broja: uređaj podržava PIN-brojeve u rasponu od 6 do 12 znamenki. Registracijom „novog “ PIN-broja automatski se „briše“ stari PIN-broj. Ukoliko se pri korištenju uređaja unese nepravilan PIN-broj 5 puta uređaj se isključuje na 3 minute te ga u tom periodu nije moguće otvoriti putem PIN-broja. U situaciji kada bi netko mogao otkriti PIN-broj može se koristiti funkcija skrivenog PIN-broja. Uređaj ima ugrađenu tehnologiju koja omogućuje prepoznavanje PIN- broja u nizu nasumično unesenih brojeva. Tipkovnica na ekranu osjetljivom na dodir postaje vidljiva samo kada se uređaj dotakne dlanom. Ova opcija pridonosi sigurnosti jer doticaj dlana briše otiske s ranije dotaknutih mjesta na uređaju i na taj način otežava otkrivanje PIN-broja.

c) Zaključavanje vrata

Uređaj Yale GATEMAN ima dva načina zaključavanja- automatsko i ručno. Kod automatskog zaključavanja uređaj putem ugrađenog senzora detektira kada su vrata zatvorena i automatski ih zaključava nakon 5 sekundi. Kod ručnog načina

zaključavanja korisnik mora pritisnuti dugme koje aktivira čitač kartice (s vanjske strane vrata) ili okrenuti polugu za ručno zaključavanje (s unutarnje strane vrata) kako bi otključao/zaključao vrata. U slučaju da su ispražnjene baterije ili je došlo do mehaničkog oštećenja uređaja također je moguće koristiti i klasičan mehanički ključ. Odabir načina rada se vrši pritiskom na dugme za odabir automatskog/manualnog načina rada koje se nalazi ispod poklopca prostora za baterije.

d) Otključavanje vrata

Uređaj koristi tri tehnologije koje omogućavaju otključavanje vrata, a to su: PIN-broj, RF-kartica i klasičan mehanički ključ.

Otključavanje vrata upotrebom PIN-broja se vrši na način da se dlanom dotakne tipkovnica kako bi se aktivirali brojevi i unese unaprijed definiran PIN-broj dužine od 6 do 12 znamenki te se još jednom dlanom dotakne tipkovnica kao potvrda unosa. Otključavanje vrata korištenjem RF-kartice se vrši na način da se RF-kartica prisloni na čitač RF-kartica ključa koji se nalazi na vanjskom modulu. Očitanje kartice traje manje od 1 sekunde. S unutarnje strane vrata otključavanje se vrši na način da se pritisne „Safehandle“ dugme i pritisne kvaka. U slučaju ispražnjenih baterija ili neke nužde moguće je koristiti polugu za mehaničko otključavanje vrata.

e) Safehandle tehnologija

Kao jedan od oblika zaštite od neovlaštenog pristupa uređaj ima ugrađenu opciju „safehandle“. Radi se o opciji koja kada je uključena zahtjeva da se prisne tipka na kvaki s unutarnje strane vrata pri otvaranju vrata. Ova tehnologija je kreirana kako bi onemogućila neovlašten pristup na način da se izbuši rupa na vratima i na prilično jednostavan način otvori vrata.

f) Onemogućavanje otključavanja vrata

U određenim situacijama se može pojaviti potreba da se onemogući otključavanje vrata s unutarnje strane. To se može napraviti na način da se RF- kartica zadrži pet sekundi na čitaču RF kartice dok se ne čuje zvučna potvrda. Kada želimo onemogućiti otključavanje vrata s vanjske strane potrebno je prekidač za onemogućavanje otključavanja prebaciti u položaj LOCK označen crvenom bojom.

Ova opcija će osigurati da se vrata ne mogu otključati s vanjske strane iako osoba ima ključ ili zna PIN-broj. Ukoliko prekidač ostane u LOCK položaju uključit će se alarm da upozori korisnika da je opcija uključena.

g) Alarm i upozorenja

Alarm od 80dB uključuje se u slučaju mehaničkog oštećenja brave ili otvaranja vrata upotrebom sile. Sigurnosti dodatno pridonosi opcija da se alarm uključuje pri detekciji temperature više od 60C stupnjeva s unutarnje strane vrata. Uređaj ima ugrađen alarmni sustav koji reagira na oštećenje uređaja, provalu, nepravilno zatvorena vrata i detekciju požara. Alarmni sustav je stalno aktivan i nisu potrebna nikakva podešavanja. Uređaj pri svakom korištenju provjerava da li su sve komponente ispravne te u slučaju detekcije bilo kakvog problema upozorava korisnika (niska razina baterije, krivo zatvorena vrata, onemogućeno otvaranje vrata s vanjske strane...). [20]

3.7 Održavanje sustava tehničke zaštite

Prema Zakonu o privatnoj zaštiti servisiranje i održavanje elemenata i konstrukcija, uređaja i sustava tehničke zaštite za objekte III. – VI. kategorije i javne površine II. i III. kategorije mora biti provedeno najmanje jednom godišnje, a servisiranje i održavanje elemenata i konstrukcija, uređaja i sustava tehničke zaštite za objekte I. i II. kategorije i javne površine I. kategorije mora biti provedeno najmanje dva puta godišnje.[35]

Poslove održavanja i servisiranja mogu obavljati pravne osobe i obrtnici koji su registrirani i ovlašteni za obavljanje poslova tehničke zaštite. Naručitelji sustava zaštite ne smiju smetnuti s uma da je održavanje i servisiranje sustava u jamstvenom roku obveza izvoditelja radova, a na zahtjev naručitelja izvoditelj je dužan ponuditi održavanje i servisiranje sustava zaštite izvan jamstvenog roka. [6]

[35]Zakon o privatnoj zaštiti (NN 16/20)

Sva sredstva, uređaji i ostala oprema koja se upotrebljavaju u zaštiti osoba i imovine moraju odgovarati hrvatskim normama, a u nedostatku hrvatskih normi, moraju odgovarati europskim normama, tj. drugim specijaliziranim normama i prihvaćenim pravilima struke. Pravne osobe i obrtnici koji su potrošači elemenata i konstrukcija, uređaja i sustava tehničke zaštite snose odgovornost za njihovu ispravnost i dužni su ih redovito održavati te servisirati najmanje jednom u godini. Vlasnik odnosno korisnik štićenog objekta obvezan je održavati u ispravnom stanju instalirani sustav tehničke zaštite kao i sve njegove pripadajuće dijelove. Poslove održavanja i servisiranja sustava tehničke zaštite mogu obavljati pravne i fizičke osobe registrirane za obavljanje poslova tehničke zaštite. Izvođač je također dužan omogućiti isporuku potrebnih pričuvnih dijelova u razdoblju pet godina od dana puštanja sustava u rad.[36]

Izvanredno održavanje

Izvanredno održavanje obavlja se na zahtjev korisnika sustava tehničke zaštite kada on ocjeni kako je takvo održavanje nužno.Vrlo često su to situacije kada je sustav odjednom prestao raditi i kada je potrebno utvrditi kada i zbog čega se to dogodilo. Ukoliko dođe do takvih situacija važno je procijeniti je li potrebno odmah reagirati, a o tome se voditelj održavanja konzultira izravno s korisnikom.[21]

Redovito održavanje

Redovito održavanje obavljase na temelju ugovora sklopljenog s korisnikom teuključuje servisiranje u unaprijed ugovorenim vremenskim intervalima. Redovito održavanje je obavezno, a ukoliko se ono ne izvrši, odnosno ne provede se u određenom roku kažnjava se novčanom kaznom jer dolazi do prekršaja. Provedba redovitih servisa uključuje aktivnosti u svim fazama procesa koji uključuju planiranje, izgradnju, obavještavanje i naposljetku naplatu. Provođenje redovitih servisa također uključuje i uobičajenu obuku korisnika za rad na ispravan način sa sustavom. Redovito održavanje se obavlja na temelju ugovora sklopljenog s korisnikom i podrazumijeva servisiranje u unaprijed dogovorenom vremenskom razdoblju i prema unaprijed dogovorenoj cijeni, a obično obuhvaća i redovitu obuku korisnika za ispravan rad. Održavanje treba predvidjeti i u jamstvenom roku. Na temelju praćenja

[36]Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN 198/2003)

rada sustava korisniku se predlaže investicijsko održavanje pri čemu se pazi na očuvanja već učinjene investicije kroz npr. korištenje i revitalizaciju već postojeće opreme.[21]

Knjige održavanja

Knjige održavanja su obavezni dokumenti koji prate poslove privatne (tehničke) zaštite i protupožarne zaštite, a glavna im je funkcija praćenje statusa sustava od dana ugradnje i tijekom cijele eksploatacije. Poslove održavanja jeizvođač radovaobvezandogovoriti sa tvrtkom ovlaštenom za poslove tehničke zaštite, a ista je obveznatemeljem ugovora izdati zapisnik o redovitom pregledu i zapisati stanja svih sustava u knjigu održavanja. [21]

4. ZAKLJUČAK

Postotak krađa i provala drastično se povećava iz godine u godinu pa se shodno tome povećava i ljudska potreba za profesionalnom zaštitom svoje imovine, bilo privatne ili poslovne. Postoje razni alarmni sustavi koji osiguravaju našu sigurnost i mir, ali ako se sustavi ne održavaju i ne servisiraju neće biti ispravni za korištenje što smanjuje njihovu učinkovitost. Upotreba protuprovalnih alarmnih sustava znatno smanjuje mogućnost otuđivanja stvari ili devastaciju ograđenog prostora, a ponekad i samo upozorenje da je objekt pod videonadzorom udalji počinitelje. Ovisno o objektu koji se štiti treba prilagoditi razinu stupnja zaštite, npr. u privatnim kućama i stanovima je dovoljno imati protuprovalna vrata, ali u prostorima koji imaju visok stupanj zaštite trebale bi se koristiti biometrijske brave zbog bolje kontrole prolaza. Nova tehnologija i novi sustavi daju nam mogućnost praćenja cijelog sustava zaštite. Na pametnom telefonu možemo pratiti situaciju dok nismo u objektu, pomoću aplikacije koja nas obavještava ukoliko su kamera ili detektori detektirali pokrete. Mislim da je u današnje vrijeme potrebno uložiti u što bolju i kvalitetniju kameru kako bi lakše identificirali počinitelja ukoliko dođe do počinjenja štete.Detektori su također nezaobilazan dio zaštite prostora koji bi trebali po mom mišljenju imati svi u svojim domovima. Svaki poslovni ili stambeni objekt bi barem trebao imati detektor dima jer su najbitniji dio sustava za dojavu požara zato što o brzini detekcije ovisi reakcija na pojavu požara, odnosno štete za prostor pa i za zdravlje ljudi.

5. LITERATURA

1. https://zastita-jukic.hr/alarmni-sustav-cuvar-vaseg-doma, pristupila 01.09.2021.,

2. https://krobel.hr/tehnicka-zastita/alarmni-sustav, pristupila 11.01.2021.,

3. https://raptor.hr/kategorija-proizvoda/tehnicka-zastita/alarmni-sustavi, pristupila 11.01.2021.,

4. .http://sigurnost-webshop.hr/https://sigurnosni-sustavi.hr, pristupila 11.01.2021.,

5. https://www.protrade-int.com/integracija-sustava, pristupila 15.01.2021.

6. DešlimunovićDavor: "Suvremeni koncepti i uređaji zaštite", I.T. Graf, Zagreb, (2002.)

7. https://www.gradimo.hr/elektrika/stupnjevi-zastite-sticenih-objekata, pristupila 15.01.221.

8. https://pimami.hr/pametne-kuce-fibaro/sistem/senzor-za-vrata-i-prozore, pristupila 15.01.2021.,

9. https://www.automatika.rs/projekti/detekcija-pokreta-primenom-pir-senzora.html, pristupila 11.01.2021.,

10.http://www.ledrasvjeta.hr/vijesti/1053-cemu-sluze-senzori.html, pristupila 17.02.2021.

11. https://www.automat-tn.hr/texecom/premier-elite-serija/detektori-pokreta.html, pristupila 17.02.2021.

12. http://peek.hr/old/index.htm pristupila 14.12.2020.

13. http://protuprovala.hr/video-nadzor pristupila 14.12.2020.

14. https://sigurnosni-sustavi.hr/kamere pristupila 17.02.2021.

15.https://poslovnasigurnost.hr/2019/02/02/poslovna-sigurnost-i-aspekti-nadzora-sustava-zastite pristupila 17.02.2021.

16. Želimir Radmilović: Stručni članak: „Biometrijska identifikacija“, Policija i sigurnost, Zagreb, (2008.)

17.https://www.prozorivrata.com/sta-je-i-kako-radi-biometrijska-brava/pristupila 16.12.2020.

18. Dešlimunović Davor.: "Menadžment zaštite i sigurnosti", Pragmatekh, Zagreb, (2006.)

19. https://1klik.com.hr/ pristupila 16.12.2020.

20. http://www.hlmcentar.hr/wp-content/uploads/2016/01/YDM-3109.pdf pristupila 16.12.2020.

21. https://www2.alarmautomatika.com/hr/odrzavanje-i-servisiranje/63/ pristupila 17.02.2021.

22. http://www.z-1.hr/videonadzor.htmlpristupila 03.09.2021.

23. Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN, 198/2003)

24. Zakon o privatnoj zaštiti (NN 16/20)

25. Zakon o zaštiti novčarskih institucija (NN 56/15,46/21)

26. Kazneni zakon (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18,126/19, 84/21)

5.1 POPIS SLIKA: