Koncept sigurnosti i proizvodnoj tvrtci

Cindrić, Ivica

Veleučilište u Karlovcu
Odjel sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Ivica Cindrić

KONCEPT SIGURNOSTI U PROIZVODNOJ TVRTCI

ZAVRŠNI RAD

Karlovac, 2018.

Karlovac University of Applied Sciences
Safety and Protection Department

Professional graduate study of Safety and Protection

Ivica Cindrić

CONCEPT OF SECURITY IN PRODUCTION COMPANY

Final paper

Karlovac, 2018.

Veleučilište u Karlovcu
Odjel sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Ivica Cindrić

KONCEPT SIGURNOSTI U PROIZVODNOJ TVRTCI

ZAVRŠNI RAD

Mentor:
dr.sc. Vladimir Tudić, prof. v.š.

Karlovac, 2018.

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.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

Stručni / **specijalistički** studij: Sigurnost i zaštita

Usmjerenje: Sigurnost i zaštita Karlovac, 02.07.2018.

ZADATAK ZAVRŠNOG RADA

Student: Ivica Cindrić Matični broj: 0422416017

Naslov: KONCEPT SIGURNOSTI U PROIZVODNOJ TVRTCI

Opis zadatka: Za potrebe Završnog rada opisati koncept tehničke zaštite odabrane proizvodne tvrtke. Također napraviti analizu radnji, postupaka i odgovornosti koje se odnose na naznačenu tematiku. Potrebno je elaborirati sve evidentne ugroze koje mogu dovesti do opasnosti, štete i neželjenog ishoda. Opisati sustav i elemente predložene tehničke zaštite te opisati naznačeni sustav u konkretnom slučaju. Odrediti tehnički prihvatljivo optimalno rješenje. U skladu s naputcima Zakona dati prijedlog mjera za povećanje sigurnosti. Koristiti stručnu literaturu, tehničke propise, proučiti Zakon, dokumentaciju proizvođača opreme. Kao podlogu za rad koristiti skice, sheme i druge dokumente sličnih projektnih zadataka. Redovito održavati konzultacije s mentorom te rad uskladiti s Pravilnikom o pisanju Završnih i Diplomskih radova Veleučilišta u Karlovcu.

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
02.07.2018.	05.09.2018.	19.09.2018.

Mentor:
dr.sc. Vladimir Tudić, prof. v.š.

Predsjednik Ispitnog povjerenstva:
mr.sc. Snježana Kirin

PREDGOVOR

Izjava

Izjavljujem da sam ovaj Završni rad napravio samostalno, koristeći znanje stečeno tijekom rada i studija, služeći se stručnom dokumentacijom i podacima tvrtke u kojoj radim i ostalom navedenom stručnom literaturom.

Zahvala

Zahvaljujem se svojoj dugogodišnjoj partnerici, Ančici Brdar, što mi je ukazala na vrijednosti daljnjeg obrazovanja i motivirala me za taj put, te mi je pomogla razviti svijest o važnosti cjeloživotnog učenja i usavršavanja. Zahvaljujem se svojoj obitelji na velikoj potpori, posebno majci. Zahvaljujem se mentoru dr.sc. Vladimiru Tudiću na savjetima, konzultacijama i pomoći pri izradi ovog završnog rada.

SAŽETAK

Koncept zaštite omogućuje efikasno smanjenje svih rizika koji proizlaze iz čimbenika sigurnosti. Konceptom zaštite utvrđuju se radnje, postupci i odgovornosti pojedinih subjekata u širokom spektru poslova sigurnosti kao što su procjena ugroženosti, tehnička zaštita, tjelesna zaštita, zaštita od požara, dostava novca, nadzor nad izvođačima, projektiranje sustava, rad nadzornog centra, upravljanje sustavom zaštite i sličnih.

Općenito se sveukupno poslovanje tvrtki u industriji vodi ekonomskom logikom što znači da će na određivanje oblika, razine i načine upravljanja sigurnošću, utjecati ekonomska logika. Prema tome potrebno je elaborirati sve moguće ugroze koji mogu dovesti do neželjenih posljedica i pronaći oblike i odrediti razinu zaštite koja će ih spriječiti ili umanjiti učinke ugrožavanja. U današnje vrijeme nemoguć je pristup udovoljavanja zakona bez traženja funkcije u djelatnosti ili kopiranje drugih rješenja koja zadovoljavaju formu. Da bi se odredilo optimalno rješenje potrebno je identificirati opasnosti, odrediti posljedice ugrožavanja, odrediti rizik i predložiti tehničko rješenje i mjeru tjelesne zaštite u svrhu smanjenja rizika na prihvatljivu razinu. Tehnička zaštita predstavlja skup radnji kojima se direktno ili posredno zaštićuju ljudi i njihova imovina, a provodi se tehničkim sredstvima i napravama te sustavima tehničke zaštite kojima je osnovna namjena sprječavanje protupravnih radnji usmjerenih prema štićenim osobama ili imovini. Sredstva i naprave tehničke zaštite su sredstva i naprave za tjelesno sprječavanje osoba u štićeni prostor ili objekt, a uz mehaničke se koriste i elektronički sigurnosni sustavi koji omogućuju kvalitetniju i prije svega učinkovitiju zaštitu štićenog objekta ili prostora.

Ključne riječi: Prosudba ugroženosti, tehnička zaštita, koncept zaštite, sustav zaštite, upravljanje sigurnošću, video nadzor, sigurnosni elaborat

SUMMARY

The concept of protection enables effective reduction of all risks arising from security factors. The concept of protection defines actions, procedures and responsibilities of individual subjects in a wide range of security affairs such as risk assessment, technical protection, physical protection, fire protection, money supply, exterminator control, system design, operation of the monitoring center, similar.

In general, the overall business of the companies in the industry is guided by economic logic, which means that the determination of the form, level and the way of security management is influenced by economic logic. Therefore, it is necessary to elaborate any possible threats that can lead to unwanted consequences and find forms and to determine the level of protection that will prevent them or reduce the effects of endangering. At present, it is impossible to access the law without looking for a function in the business or copying other solutions that conform to the form. In order to determine the optimal solution, it is necessary to identify the dangers, determine the consequences of the risk, determine the risk and propose a technical solution and measure of physical protection to reduce the risk to an acceptable level. Technical protection is a set of actions that directly or indirectly protect people and their property and are implemented through technical means and devices and systems of technical protection which are the primary purpose of preventing unlawful acts directed at protected persons or property. Means and devices of technical protection are means and devices for the physical prevention of persons in a protected space or facility, and with the use of mechanical electronic security systems that enable better quality and, above all, more effective protection of the protected object or space.

Key words: Judgment of threat, technical protection, concept of protection, system protection, security management, video surveillance, security elaboration

SADRŽAJ

1. UVOD

Sigurnost je jedna od najaktualnijih tema u poslovnom svijetu posebno za one uspješne poslovne pojedince i tvrtke koje smatraju da se za uspjeh dovoljno baviti isključivo svojim vlastitim poslom. Iako većina poslovnih ljudi i dalje razmišlja na taj način, ne smijemo isključiti činjenicu da je globalni porast životnih troškova u svoje cijene uključio i faktor nesigurnosti te mogućnost novih prijetnji i ugrožavanja. Tiče li se to manjih naroda jednako kao i velikih, odavno je postalo bespredmetno pitanje, praktično od onog trenutka kada se svijet globalno počeo povezivati.

Promjene koje se sve brže događaju u sferi gospodarskih odnosa reflektiraju se na razvoj zaštitarskog tržišta. Svaki sustav tehničke zaštite nakon izvedbe i primjene mjera tjelesne zaštite svoju potpunu funkcionalnost postiže nakon primopredaje sustava s korisnikom. Pri tome važnost edukacije korisnika sustava dolazi sve više u prvi plan zbog kompleksnosti sustava i primjene sve složenijih mjera zaštite bez obzira na isticanje proizvođača da su njihovi proizvodi jednostavni i okrenuti krajnjem korisniku. Od zaštitara se očekuje da su osposobljeni i upućeni za rad s najnovijim uređajima i metodama štićenja, a da pri tome njihova cijena usluge financijski ne opterećuje previše poslovanje. Zaštitari će vam reći da je sve izvedivo, ali odgovarajuća zaštita ima svoju cijenu bez obzira što cijene uređaja i opreme neprekidno padaju, a njihove se mogućnosti primjene povećavaju. U našoj zemlji situacija se u zaštitarstvu pozitivno mijenja i zaštitari su napravili pomak koji je mjerljiv u kvaliteti pružene usluge, ali se čeka jači gospodarski rast koji će dati pravi poticaj razvoju zaštitarskog tržišta. Zaštitari na nadzornim kamerama imaju važnu ulogu u smislu "reagiranja" na štetan događaj, a stručnjaci sigurnosti da im ukažu gdje je moguće nastajanje tog štetnog događaja i na koji način.

1.1. Predmet i cilj rada

Upotreba tehničke zaštite pri osiguravanju proizvodnih tvrtki raznih industrija sve je veća te se javlja potreba za konceptualnim rješenjima koje sjedinjuju sve sustave zaštite. Rješenja bi trebala biti jednaka za svakog tko ulaže u osiguranje, a u skladu je sa zahtjevima i financijskim planovima organizacije. Koncept zaštite kao formalni akt će omogućiti stručnjacima za sigurnost lakše praćenje i nadopunjavanje zaštite svoje tvrtke. Koncept će sadržavati sve navedene ugroze i načine kako ih što efikasnije spriječiti. Koncept mora biti tako konstruiran da nametne standard pri samom projektiranju, izvođenju i nadzoru te kasnijoj reviziji i održavanju svih segmenata zaštite.

Koncept se temelji na sljedećem:

- trenutno važećoj zakonskoj regulativi za predmetno područje
- trenutno važećim zahtjevima osiguravajućih kuća
- razini kriminaliteta u državi
- pratećem tehnološkom nivou
- radnim procesima u proizvodnom pogonu
- saznanjima o štetnim događanjima unutar tvrtke
- prostornom smještaju funkcionalnih zgrada unutar tvrtke

Uz navedene standarde, koncept mora biti sukladan zakonskom regulativom i biti ažuran u svakom trenutku sa svakom promjenom unutar tvrtke ili sa promjenama zakonske regulative. Na tržištu postoje konkurentske tvrtke raznih izvođača i opreme stoga koncept mora osigurati brzu i laku promjenu partnera ugovorenog za poslove tehničke zaštite. Kako je bitan formalni koncept zaštite tako i njegova pravovremena revizija ili analiza na osnovu koje se on može uvijek ažurirati sa najnovijom regulativom, a također i sa primjenom najnovijih tehnologija. Ovim radom dan je primjer zaštite proizvodne tvrtke kroz izradu prosudbe ugroženosti i procesa analize koji kreće od same regulative, zatim pregleda postojećih sustava u objektu te na kraju završna ocjena stanja sigurnosti i prijedlogom budućih mjera za poboljšanje te završava zaključkom.

Svaka proizvodna tvrtka često ima ograničena financijska sredstva za određeno područje tako i za područje tehničke zaštite. Zato je potrebno planiranje zaštite kroz koncept i osiguranje sredstava za implementaciju svih sustava zaštite, po mogućnosti na vrijeme planirati i rezervirati. Menadžer u tvrtci mora se baviti financijskim aspektom sigurnosti zbog ograničenih sredstava uz koje mora zadovoljiti zahtijeve za sigurnošću. Zato bi trebao biti što više pozicioniran u strukturi tvrtke te odgovoran samo upravi.

Cilj završnog rada je ukazati na potrebu planiranja zaštite kroz postavljanje koncepta zaštite, te izrade prosudbe ugroženosti koji prati sve bitne čimbenike vezane uz zaštitu osoba i imovine. Koncept zaštite podrazumijeva formalni akt kao prilog ugovoru sa kasnijim strateškim partnerima za poslove sigurnosti. Osim sustavnog ažuriranja istog potrebno je svakih nekoliko godina zatražiti analizu koncepta i svih njegovih posljedičnih veza. Tako je potrebno provjeriti i stanje na terenu na objektima, je li se poštivao ugovoreni koncept i koja su odstupanja. Važno je u postavljanje normativa i prosudbu ugroženosti izraditi po pravilima struke, a još je važnije da se sustavno prate promjene u poslovnim procesima, stanje u zakonodavstvu i općenito stanje sigurnosti u regiji i sukladno tome ažurira koncept kako bi uvijek bila postignuta optimalna zaštita. Za pravilnu analizu ili reviziju jako je bitno ovaj posao povjeriti potpuno neovisnoj pravnoj osobi kako bi dobili stvarno stanje sigurnosti.

1.3. Izvori podataka i metode prikupljanja

Za izradu Završnog rada korištena je stručna literatura i dostupne internetske stranice, studij dokumentacije, sistemsko promatranje te trenutačno zapažanje. Studij dokumentacije znači prikupljanje, analiza i obrada podataka. Podaci su prikupljeni temeljitim pregledom i analizom raspoložive dokumentacije, kao i obilaskom objekta. U istraživanju se pošlo od toga što je prosudba ugroženosti, koji je koncept zaštite, kako je on formiran, na koji način je implementiran u praksi, te koji su propusti i moguće nadogradnje istog, da se osigura optimalan nivo zaštite u skladu sa zakonskim okvirima.

2. TEORIJSKI DIO

Poduzetnici se u svom poslovanju, osim s raznim preprekama, susreću i s krađama, kako od nepoznatih osoba tako i od radnika. Pod radnicima se smatra sve zaposlenike bez obzira na funkciju koju obavljaju i vrstu ugovora koji imaju s poslodavcem: o radu, menadžerski, o djelu, studentski ili sličan ugovor. Krađe općenito, a tako i krađe radnika mogli bismo podijeliti na tri vrste:

- jednostavne,
- kompleksne
- sofisticirane.

U jednostavne krađe možemo svrstati krađu robe/materijala sa skladišta ili trgovine poslodavca, krađu uredskog materijala, sredstava za čišćenje i higijenskog pribora, naplatu od kupca za svoj račun, upotrebu opreme i resursa poslodavca za vlastiti račun. Kompleksnije krađe su one koje najčešće uključuju dobavljače robe i usluga, a to su potvrđivanje preuzimanja robe dobavljaču mada nije dostavljena, te ovjera računa za koje poslovi nisu obavljeni. Nakon takvih radnji dobavljač i radnik podijele protupravno stečen novac, a poslodavac je znatno oštećen. Kompleksnije krađe su i pronevjere. U pronevjerama novac se najčešće prenosi na račune koji nisu poslovni računi dobavljača, a u poslovnim knjigama prijenosi sredstava prikazuju se kao plaćanje obveza prema dobavljačima ili se prikazuju fiktivni troškovi kao troškovi prilikom obavljanja obveza iz ugovora o radu, kao npr. putni nalozi koji se podnose poslodavcu. Sofisticirane krađe ulaze u domenu poslovne špijunaže i to su prodaje baza kupaca konkurenciji, krađa i odavanje poslovnih tajni konkurenciji, preusmjeravanje kupaca konkurenciji. One se ujedno i najteže otkrivaju, a znaju dovesti do ogromnih šteta za poduzetnika, čak i do propasti. Dokazivanje odgovornosti kod tih krađa teško je, ako kod poduzetnika nije jasno određeno tko ima pristup kojim informacijama te ako nisu uvedene mjere za praćenje kopiranja i distribuiranja podataka.

2.1. Dokazivanje kao složeni postupak

Bez obzira na to s kakvim se vrstama krađa susreće poduzetnik, nužno je uspostaviti sve kontrolne mjere u svrhu otkrivanja i sprječavanja krađa koje stoje na raspolaganju poduzetniku. Praksa pokazuje da su u društvima koja imaju mjere sprječavanja rizika od krađe, krađe manje prisutne. Te mjere također pomažu u otkrivanju odgovornih osoba za krađe kao i u dokaznom postupku protiv odgovornih osoba. Naime, naknada štete poduzetniku koji je pretrpio štetu nije moguća bez provođenja dokaznog postupka, osim u slučaju priznanja i nagodbe s osobom odgovornom za krađu. Prilikom donošenja mjera potrebno je obratiti pozornost na odredbe Zakona o zaštiti osobnih podataka te da se uvedenim mjerama ne krše prava na privatnost radnika. Zakonski propisi nalažu da, ako se radnici snimaju tijekom radnih procesa, to mora biti jasno naznačeno na ulazu u radne prostorije ili bi se to smatralo nedopuštenim snimanjem radnika. Poduzetnici bi trebali svoje radnike izvijestiti prilikom otvaranja računa za elektroničku poštu da poslodavac ima pravo pregledavati elektroničku poštu koja pristiže i odašilja se s poslovnog računa. Poduzetnik bi također trebao donijeti interni pravilnik o poslovnoj tajni kako bi se osobama koje barataju poslovnim podacima i koje imaju pristup poslovnim informacijama jasno iznijelo koji se podaci smiju kome i na koji način distribuirati. Ako taj pravilnik postoji, olakšani su dokazivanje odavanja poslovne tajne i naplata nastale štete od odgovornih osoba. Opće odredbe o poslovnoj tajni navedene u ugovoru o radu ili menadžerskom ugovoru često nisu dovoljne da bi se sa sigurnošću ustvrdilo da je radnik bio upoznat s činjenicom da neke podatke ne smije otkrivati neovlaštenim osobama, pa se zahtjevi za naknadu štete često odbacuju. Pronevjere se najčešće sprječavaju propisivanjem postupka plaćanja i određivanjem limita za samostalno potpisivanje naloga platnog prometa i stalnim usporedbama i usklađenjima stanja s dobavljačima.

Tab1. Prikaz odabira internih sredstava poslodavca

ODABIR INTERNIH SREDSTAVA	
Jednostavne krađe	· razgovori s radnicima koji rade ili su zaduženi za predmet krađe · pregledavanje snimki kamera · utvrđivanje manjka robe/materijala/inventara
Kompleksnije krađe	· razgovori s radnicima koji sudjeluju u poslovnim procesima u kojima je krađa otkrivena · pregledavanje snimki kamera · pregled komunikacije obavljane putem poslovne elektroničke pošte · interna revizija poslovne dokumentacije o zaprimanju robe i/ili usluga · interna revizija stanja dobavljača uz usklađenje s dobavljačima · komunikacija s dobavljačima · komunikacija s kupcima
Sofisticirane krađe	· razgovori s radnicima koji imaju pristup podacima koji su postali dostupni konkurenciji, a nisu javno dostupni · pregledavanje snimki kamera ako je primjenjivo · pregled komunikacije obavljane putem poslovne elektroničke pošte · pregled slanja podataka s IP adresa · pregled snimanja podataka

Kada se krađa otkrije, poduzetnik se nađe pred izazovom kako otkriti osobe odgovorne za nju i nastalu štetu, kako dokazati odgovornost te u konačnici kako naplatiti štetu.

2.2. Pet uobičajnih osobina osoba koje treba nadzirati

Međunarodna osiguravajuća kuća Hiscox je identificirala pet uobičajenih osobina osoba koje treba nadzirati:

Inteligentni i znatiželjni: prevaranti i lopovi često žele znati kako sve funkcionira u tvrtci u kojoj rade. Kad nauče proces rada, veoma su sposobni da njime manipuliraju za postizanje vlastite koristi.

Ekstravagant: treba pripaziti na radnika čiji način života nije proporcionalan njegovoj plaći.

Sklon riziku: onaj koji se bavi prevarama i pronevjerom često ne poštuje pravila i nije radišan radnik. Često je sklon ekstremnim akcijama – od prebrze vožnje auta do pretjeranog korištenja bolovanja.

Duhoviti i ambiciozni: onaj koji je sklon pronevjerama i krađi često odluči dolaziti ranije na posao ili ostajati do kasno. Često se predstavlja predan firmi za koju radi, a zapravo nastoji da ne bude uhvaćen.

Nezadovoljni: zaposleni koji osjeća da se prema njemu ne postupa sa poštovanjem, može biti u iskušenju počiniti krađu radi "osvete" prema nadležnima. Ponekad su te osobe veoma nervozne, sa čestim promjenama u ponašanju.

2.3. Izvanredni otkaz

Bez obzira o kakvoj je krađi riječ, svaka od njih nanosi štetu poduzetniku. Ako je počinitelj radnik, ta krađa nepovratno narušava povjerenje poslodavca prema radniku, što dovodi do izvanrednog otkaza ugovora o radu. Često je to nepopularna tema, posebno kod manjih krađa. Naime, u komentarima ispod članaka često se staje na stranu radnika koji je dobio otkaz zbog ‘zanemarive’ krađe od poslodavca. Odmah se počinju spominjati uvjeti koje su ugovorili poslodavac i radnik, kako je radnik bio potplaćen, te da nije imao drugog izbora nego potkradati poslodavca, da tako i treba i sl. Pritom se zaboravlja da su poslodavac i radnik sklopili određeni ugovor o radu i da su ga se obje strane dužne pridržavati i to ne samo nekih odredbi. Prema Zakonu o radu radniku je moguće izvanredno otkazati ugovor o radu zbog osobito teške povrede obveze iz radnog odnosa ili neke druge važne činjenice zbog koje nastavak radnog odnosa nije moguć. Smatram da je krađa od poslodavca vrlo važna činjenica zbog koje nastavak radnog odnosa nije moguć. Kod krađe je definitivno svako povjerenje između poslodavca i radnika nepovratno narušeno i otkaz kod dokazane krađe je neizbježan osim, ako poslodavac uvaži neke okolnosti koje opravdavaju radnika te svojom procjenom utvrdi da je to izolirani slučaj koji se više neće ponavljati. Poslodavac je dužan u roku od 15 dana od saznavanja činjenica radniku uručiti otkaz. U tom otkazu potrebno je dobro obrazložiti koje su činjenice dovele do izvanrednog otkazivanja ugovora o radu te pružiti radniku mogućnost na pravni lijek (zahtjev za zaštitu prava) u roku od 15 dana. Česta je situacija da radnik u takvim situacijama odbija primiti otkaz. Prema

odredbama Zakona o parničnom postupku, tada se otkaz uručuje preporučenom poštom s povratnicom na adresu prebivališta ili boravišta radnika. Ako je ta dostava neuspjela, dostava otkaza se prema odredbama istog zakona obavlja putem oglasne ploče poslodavca i smatra se obavljenom nakon isteka roka od osam dana od postavljanja otkaza na oglasnu ploču. Osim izvanrednog otkaza ugovora o radu, česta je situacija da se kod otkazivanja ugovora o radu zbog krađe sklapa sporazum o raskidu ugovora o radu koji uključuje i naknadu štete. U ovoj situacije važno je imati na umu da se sporazum treba postići u roku od 15 dana od saznavanja činjenica koje su razlog za izvanredni otkaz kako se ne bi izgubila mogućnost davanja izvanrednog otkaza počinitelju krađe.

2.4. Regulativa za sustave tehničke zaštite

Kao što je navedeno ranije, ovo istraživanje započeto je sa regulativom tj. pregledom propisa koji pravno reguliraju ovo područje. Najvažniji propisi su:

- Zakon o privatnoj zaštiti (NN 68/03., 31/10., 139/10.)
- Kazneni zakon (NN 125/11.)
- Zakon o tajnosti podataka (NN 79/07., 86/12.)
- Zakon o informacijskoj sigurnosti (NN 79/07.)
- Zakon o sprječavanju nereda na sportskim natjecanjima (NN 117/03., 71/06., 43/09., 34/11.)
- Zakon o kritičnim infrastrukturama (NN 56/13.)
- Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN 198/03.)
- Pravilnik o načinu i uvjetima obavljanja poslova privatne zaštite na javnim površinama (NN 36/12).
- zakon o gradnji (NN175/03)
- zakon o zaštiti na radu (NN 114/03)
- zakon o zaštiti od požara (NN 58/93)

2.5. Stupnjevi zaštite

Po zakonu o privatnoj zaštiti obveza je svih vlasnika sustava izraditi prosudbu ugroženosti i sigurnosni elaborat u kojem se također objekt mora svrstati u neku

od kategorija ugroženosti. Postoji 6 kategorija ugroženosti objekta, a za svaku su propisane obavezne mjere zaštite:

I. kategorija - NAJVIŠI STUPANJ ZAŠTITE koji predviđa:

- mehaničku i tehničku zaštitu kojom se signalizira neovlašten ulazak u štićeni prostor i dojavljuje na CDS (Centralno dojavni sustav),
- tehničku zaštitu kojom se prati kretanje u štićenom prostoru i pojedinačno štićenim prostorijama (kontrola prolaza i video nadzor) uz video zapis,
- zaštitu pojedinačnih vrijednosti pomoću specijalnih kasa, trezora i sl.,
- integralnu zaštitu s najmanje jednim lokalnim nadzornim mjestom i sustavom veze sa zaštitarima na štićenom objektu,
- sigurnosni plan postupanja i procedure u slučajevima pretpostavljenih incidentnih situacija.

II. kategorija - VISOKI STUPANJ ZAŠTITE koji predviđa:

- mehaničku i tehničku zaštitu kojom se signalizira neovlašten ulazak u štićeni prostor i dojavljuje na CDS,
- tehničku zaštitu kojom se prati kretanje u štićenom prostoru (kontrola prolaza i video nadzor) uz video zapis,
- integralnu zaštitu s najmanje jednim lokalnim nadzornim mjestom i sustavom veze sa CDS-om.

III. kategorija - VIŠI STUPANJ ZAŠTITE koji predviđa:

- mehaničku i tehničku zaštitu kojom se signalizira neovlašten ulazak u štićeni prostor i dojavljuje na CDS,
- tehničku zaštitu kojom se prati kretanje u štićenom prostoru (kontrola prolaza i video nadzor) uz video zapis.

IV. kategorija - SREDNJI STUPANJ ZAŠTITE koji predviđa:

- mehaničku i tehničku zaštitu kojom se na licu mjesta zvučno ili svjetlosno signalizira neovlašten ulazak u štićeni prostor,
- video nadzor kojim se prati kretanje u štićenom prostoru uz video zapis.

V. kategorija - NIŽI STUPANJ ZAŠTITE koji predviđa:

- mehaničku i tehničku zaštitu kojom se na licu mjesta zvučno ili svjetlosno signalizira neovlašten ulazak u štićeni prostor,

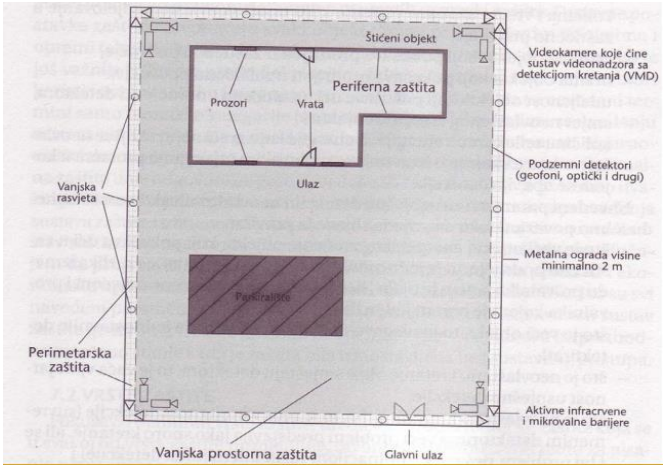
VI. kategorija - MINIMUM ZAŠTITE koji predviđa:

- mehaničku zaštitu bez uporabe elektroničkih naprava,
- obične cilindarske brave,
- obične ograde bez tehničkih elemenata

2.6. Vrste zaštite

Pošto u svakom štićenom prostoru ili objektu postoji više zona koje je potrebno nadzirati, shodno tome postoje i različite vrste zaštite, a to su:

1.perimetarska zaštita
2.vanjska prostorna zaštita
3.periferna zaštita
4.unutarnja prostorna zaštita
5.zaštita štićenog predmeta



Slika 1. Predodžba perimetarske, vanjske prostorne i periferne zaštite

1) Perimetarska zaštita nalazi se na liniji razdvajanja između vanjske nezaštićene zone i zaštićenog prostora. Nezaštićena zona može biti nadzirana,

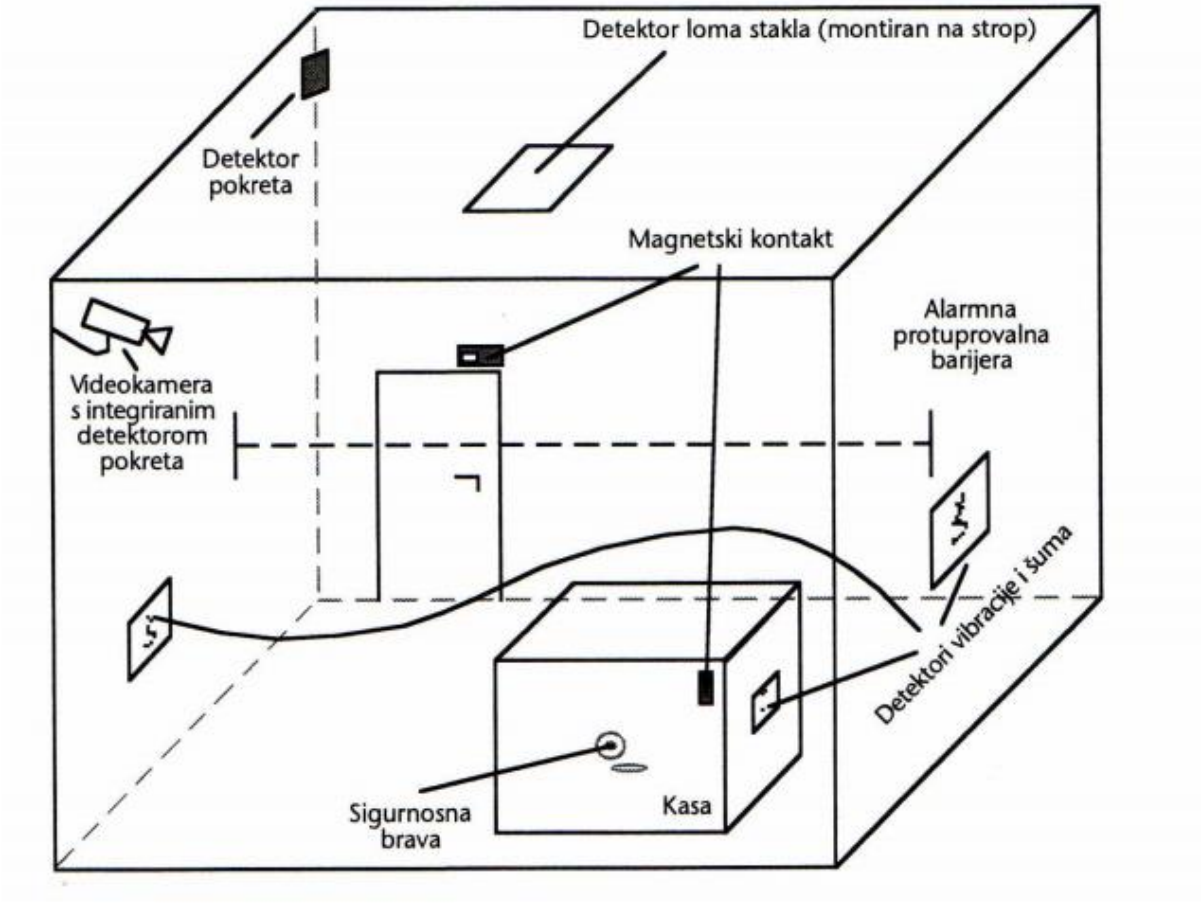
ali tu zaštitarska služba koja je zadužena za tjelesnu zaštitu na štićenom objektu nema nadležnosti. Perimetarska zaštita je ,,prva linija obrane" štićenog objekta, najčešće ju predstavlja ograda koja mora omogućiti detekciju pokušaja ulaska u zaštićeno područje. Perimetarska zaštita je prva vrsta zaštite ili prsten sigurnosti koji zahtjeva određenu infrastrukturu pri implementaciji kao što su vanjske ograde, pregrade i zidovi, razne prirodne i umjetne prepreke u kombinaciji sa sustavima tehničke zaštite.

2) Vanjska prostorna zaštita se odnosi na područje štićenja koje se nalazi između perimetarske i periferne zaštite. Za vanjsku prostornu zaštitu važne karakteristike su položaj, veličina te preglednost. Preporuka za taj dio zaštićenog prostora je ta da se taj dio prostora očisti od prirodne vegetacije i umjetno izgrađenih prepreka. Važno je redovno čistiti vegetaciju kako ne bi dolazilo do aktiviranja lažnih alarma te smanjenja vjerojatnosti otkrivanja neovlaštenih ulaska.

3) Periferna zaštita predstavlja perifernu zaštitu štićenog objekta. To znači da se periferna zaštita odnosi na zaštitu svih vrata, prozora, zidova ili jednostavnije rečeno svih otvora koji se nalaze u štićenom objektu. Ukoliko je periferna zaštita ispravno projektirana i izvedena, ne smije se aktivirati prilikom neovlaštenog kretanja ili bilo koje druge protupravne aktivnosti koja se događa izvan ili unutar štićenog objekta, jer su ta područja nadzirana drugim vrstama zaštite. Ne smije se dogoditi situacija u kojoj će nakon aktiviranja periferne zaštite na licu mjesta pojaviti vanjska zaštitarska služba, jer je za taj dio zadužena unutarnja zaštitarska služba. Također perimetarska zaštita ne smije se aktivirati, ako je kretanje izvan objekta štićenja. Uspostava periferne zaštite ne smije narušavati mogućnost slobodnog kretanja unutar i izvan štićenog objekta, a uređaji koji se primjenjuju mogu biti smješteni u području vanjske ili unutarnje prostorne zaštite.

4) Prostor unutar periferne zaštite se nalazi u području unutarnje prostorne zaštite. Djelovanje ove vrsta zaštite usmjereno je na detekciju neovlaštenih

aktivnosti unutar štićenog objekta u prostoru između periferne zaštite i zaštite samog štićenog objekta. Saznanje da je svaki dio unutar štićenog prostora nadziran ima snažan preventivni učinak. Važan zahtjev koji se postavlja pred unutarnju prostornu zaštitu je mogućnost djelomičnog uključenja i isključenja zaštite u različitim djelovima objekta čime se definira mogućnost točnije detekcije neovlaštenog djelovanja. Sve vrste zaštita moraju u najmanjoj mogućoj mjeri narušavati uobičajno obavljanje poslovnog procesa.



Slika 2. Predodžba unutarnje prostorne zaštite i zaštita štićenog objekta

5) Zaštita štićenog objekta predstavlja zadnji prsten sigurnosti. Zbog vrijednosti i važnosti štićenog objekta se postavljaju svi prethodni stupnjevi. Cilj ove zaštite je da se detektira, prenese i signalizira svako neovlašteno djelovanje koje ima za cilj oštećenje ili otuđenje štićenog predmeta. Aktiviranje alarma je trenutno, jer se na taj način skraćuje vrijeme potrebno za intervenciju i povećava

vjerojatnost za sprječavanje štetnog djelovanja. Univerzalno pravilo u zaštiti i sigurnosti ukazuje da optimalni sustav zaštite nije moguće ostvariti primjenom samo jedne vrste zaštite, nego se optimalna zaštita uspostavlja uvijek primjenom više različitih vrsta i stupnjeva zaštite.

2.7. Mehanička zaštita

Mehanička zaštita je oblik zaštite čije su karakteristike nedovoljno korištene pri izradi projekata sustava zaštite. Razlog tomu je ne poznavanje svih elemenata mehaničke zaštite i podcjenjivanje njene mogućnosti. Mehanička zaštita je preteča svih vrsta zaštita. Od davnina čovjek koristi prirodne prepreke i barijere za izgradnju i zaštitu svog doma. Razvojem tehnologije izrade materijala povećane su mogućnosti primjene mehaničke zaštite za najsloženije sustave zaštite. Projektanti prilikom projektiranja sustava zaštite obavezno imaju konzultacije sa građevinskim stručnjacima i arhitektima. Zbog smještaja i veličine štićenog objekta nije moguće uvijek postići maksimalni stupanj zaštite.

Slika 3. Predodžba rampe

Mehaničkom zaštitom se sprječava slučajan ili namjeran ulazak u štićeni prostor ili se usmjerava na mjesto ili put kretanja koji nije pod zabranom. Osim za ljude, ova vrsta zaštite se primjenjuje i na vozila, primjerice rampe kao što je prikazano na slici (slika 3).

Sustavom mehaničke zaštite se smatraju:

- rešetke

- barijere
- rampe
- protuprovalna vrata
- protuprovalne brave
- neprobojna stakla
- sefovi
- trezori
- ograda

Ograda je prvi element mehaničke zaštite koji ima sljedeće funkcije:

1. Ograda omeđuje određeno područje
2. Sprječava namjeran ili slučajan ulazak u zaštićeno područje
3. Djeluje kao regulator kretanja osoba i vozila

Parametri prije postavljanja ograde:

1. da li je potrebno postaviti posebne barijere za sprječavanje nasilnog ulaska vozila
2. da li će za sprječavanje nasilnog ulaska biti dovoljna jedna ili više ograda, te ukoliko je odgovor da, koje visine i na kojem razmaku ih je potrebno postaviti
3. koliko daleko mora biti postavljena ograda obzirom na udaljenost od štićene građevine
4. da li ograda kao element mehaničke zaštite mora djelovati sa sustavom tehničke zaštite i da li se svaki neovlašteni pokušaj ulaska mora registrirati i izazvati alarmno stanje
5. prema specifičnim uvjetima okoline koje prirodne prepreke mogu olakšati ili onemogućiti sposobnost detekcije duž cijele ograde

2.7.1. Protuprovalna vrata

Protuprovalna vrata su vrata velike mase (do nekoliko stotina kilograma), veće debljine, čvrstoće i izdržljivosti, učvršćene sa više točaka učvršćivanja u okvir. Svaka kvalitetna protuprovalna vrata moraju sadržavati ovih pet elemenata:

1. Protuprovalno krilo - sadrži troslojni čelični lim debljine 2-3 mm, srednji sloj služi za održavanje ravnine vrata pomoću rešetke, čelične mreže ili perforiranog lima. Mogu biti dodani toplinski, zvučni i protubalistički slojevi, a između slojeva se nalaze kvarcni pijesak i keramički materijali.
2. Protuprovalni dovratnik - napravljen je od višeslojnog lima 2-3 mm debljine zavarenih spojeva. Spoj sa zidom je pomoću sidrenih zidnih vijaka 6-8 komada duljine 2,5 cm. Ispuna između dovratnika i zida je beton, a dovratnik ima rupe kao sjedište za šipke i klinove.
3. Protuprovalni okovi - onemogućuju podizanje krila i izbijanje vrata te su potrebna minimalno tri okova na vratima.
4. Protuprovalna brava- sadrži kodirani ključ i 3-5 šipki
5. Protuprovalne šipke i zasune - razlikuju sa aktivne i pasivne šipke u krilu. Aktivne šipke se pokreću sa ključem, a pasivne šipke nalazimo na djelu krila gdje su okovi.

Svaka vrata mogu imati tri radna stanja:
- otvorena
- zatvorena
- zabravljena

Jedino zabravljena vrata imaju peti element protuprovale. Mehanička zaštita predstavlja neizostavan element svakog sustava zaštite, a praksa je pokazala da se najveća važnost mehaničkoj zaštiti pridaje upravo pri projektiranju sustava zaštite koji moraju zadovoljiti najviše sigurnosne standarde i maksimalni stupanj zaštite.

2.8. Tehnička zaštita

Kvalitetno projektirana mehanička zaštita se u mnogo slučajeva pokazala jednom od najvažnijih elemenata zaštite, no napretkom tehnologije i sve većom potrebom za kvalitetniju zaštitu štićenih prostora ili objekata razvija se tehnička zaštita. Tehnička zaštita predstavlja skup radnji kojima se neposredno ili posredno zaštićuju ljudi i njihova imovina, a provodi se tehničkim sredstvima i napravama te sustavima tehničke zaštite kojima je osnovna namjena sprečavanje protuprovalnih radnji usmjerenih prema štićenim osobama ili imovini. Tehničku zaštitu djelimo u tri kategorije:

1) protuprepadno
2) protuprovalno
3) protusabotažno

1) Protuprepadnom zaštitom se pokušava provalnika osujetiti, odvratiti od štetnih događaja. Ova kategorija je najjeftinija kategorija tehnička zaštite, a obuhvaća natpise, naljepnice (slika 4), digitalne špijunke (slika 5) i fotoaparat.

Slika 4. Predodžba naljepnice

Slika 5. Predodžba digitalne špijunke

2) Protuprovalnom zaštitom se pokušava zaustaviti i spriječiti ulaz u štićeni prostor zaprekama ili elektoničkim elementima tehničke zaštite. Za ovakvu zaštitu postoje sustavi mahaničke zaštite (slika 6) i sustavi video nadzora sa postojećim elektroničkim elementima koji su međusobno povezani sa centralom.

Slika 6. Predodžba barijere

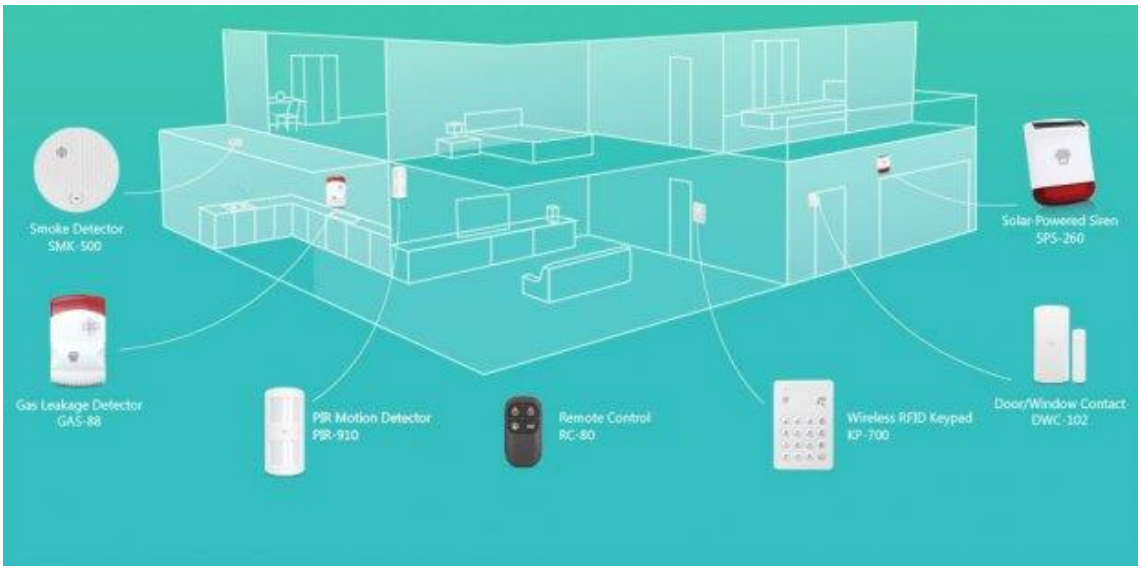
3) Protusabotažnom zaštitom kao što sama riječ opisuje, pokušava se spriječiti sabotaža postojećeg sustava. Primjeri kao što je postavljanje kamere na visini da je provalnik ne može uništiti, sakrivanjem centrale u zid, osiguranje dodatnog napajanja ukoliko provalnik uspije isključiti struju u štićenom objektu, skrivene kamere (slika 7.) i sl.

Slika 7. Predodžba snimke skrivene kamere

2.9. Protuprovalni sustav

Protuprovalni sustav je predviđen za detekciju i registraciju svakog neovlaštenog ulaska u štićeni prostor. Nakon njihova aktiviranja potrebno je prenjeti žičanim ili bežičnim putem alarmni signal o vrsti i točnoj lokaciji detektiranog neovlaštenog kretanja u lokalnu nadzornu sobu i/ili u udaljeni centralni dojavni sustav. Uređaji koji se koriste u protuprovalnim sustavima zaštite kao i svi ostali elektronički uređaji tehničke zaštite zahvaljujući ubrzanom rastu elektronske industrije nude sve više tehničkih mogućnosti i "inteligentnija" rješenja za manju cijenu. Uz klasične žičane protuprovalne sustave zaštite sve se više koriste bežični alarmni sustavi. Bežični prijenos signala se najviše koristi za:

- kućnu elektroniku (portafon, bežični mikrofon, uređaj za lokalni prijenos signala i sl.)
- računarske opreme za bežične LAN (Local Area Network) mreže koje koriste standard IEEE. 802.11 za prijenos podataka u lokalnim računarskim mrežama do 100 metara pri brzini 2 Mbps
- bluetooth uređaji



Slika 8. Predodžba bežičnog alarmnog sustava

Međunarodni standard IEEE 802.11 je prihvaćen u cijelom svijetu za prijenos podataka u lokalnim računarskim mrežama pa je zbog toga prihvatljiv i za bežični prijenos alarmnih informacija u digitalnom obliku. Bluetooth standard je popularan i raširen zbog praktičnosti i pouzdanog prijenosa, a razvio se napredni standard koji uključuje enkripciju podataka i promjenu frekvencije prijenosa do 1600 puta u sekundi (frequncy hopping) što ga čini pouzdanim u bežičnim alarmnim sustavima. U početku se bežični prijenos podataka manje koristio zbog sljedećih razloga:

1. morao je biti omogućen pouzdan i zaštićen prijenos podataka. Današnji bežični sustavi omogućavaju digitalni prijenos signala koji je kodiran i koristi FH (frequency hopping) te je na taj način dovoljno zaštićen
2. prvi bežični detektori su imali relativno veliku potrošnju energije te im je bilo potrebno često mjenjati baterije.

3. suvremeni bežični detektori imaju mogućnost uključenja i u tom slučaju prijenosa signala do prijamnika u štedljivom modu koji smanjuje broj prijenosa signala ukoliko cjelokupni alarmni sustav nije uključen

Danas se puno više koriste bežični alarmni sustavi, jer su napretkom tehnologije navedeni razlozi otklonjeni. Iako je sustav sa bežičnom vezom puno jednostavnije instalirati, ipak postoje nedostatci:
- moguće preslušavanje kanala i dekodiranje zapisa
- moguće kloniranje signala i sabotaža wireless (bežičnog) sustava
- načelo komunikacije u bežičnom sustavu je to da se detektori "uparuju" sa centralom. Problem kod uparivnja je taj da ako dođe do gubitka napona, onda je potrebno ponovno uparivanje pojedinog detektora.

Protuprovalni sustav dobro je kombinirati s mehaničkim sredstvima zaštite u svrhu produženja vremena potrebnog za provalu do intervencije tjelesne zaštite. Osnovni elementi protuprovalnog sustava su alarmna centrala, upravljački paneli, detektori i sredstva za uzbunjivanje i dojavu. Prema načinu spajanja detektora na alarmnu centralu razlikujemo dvije vrste sustava:
1. konvencionalni sustav protuprovale
2. adresabilni sustav protuprovale

Kod konvencionalnih sustava protuprovale detektori se spajaju na alarmne zone. Na matičnim pločama većina alarmnih centrala ugrađen je određen broj alarmnih zona, a naknadno povećanje broja zona ostvaruje se ugradnjom dodatnih modula na matičnu ploču. Alarmni moduli nadziru rad detektora i konstantnom komunikacijom sa centralnim uređajem dojavljuju status svakog detektora. Na jedan alarmni modul može de spojiti do četiri, osam ili šesnaest detektora, ovisno o tipu modula. Alarmni modul provjerava naponske razine na alarmnim ulazima. Svaka naponska razina na alarmnom ulazu odgovara nekom od ova četiri stanja:
1. sabotaža / prekinuta linija
2. normalno stanje

3. alarmno stanje
4. linija u kratkom spoju

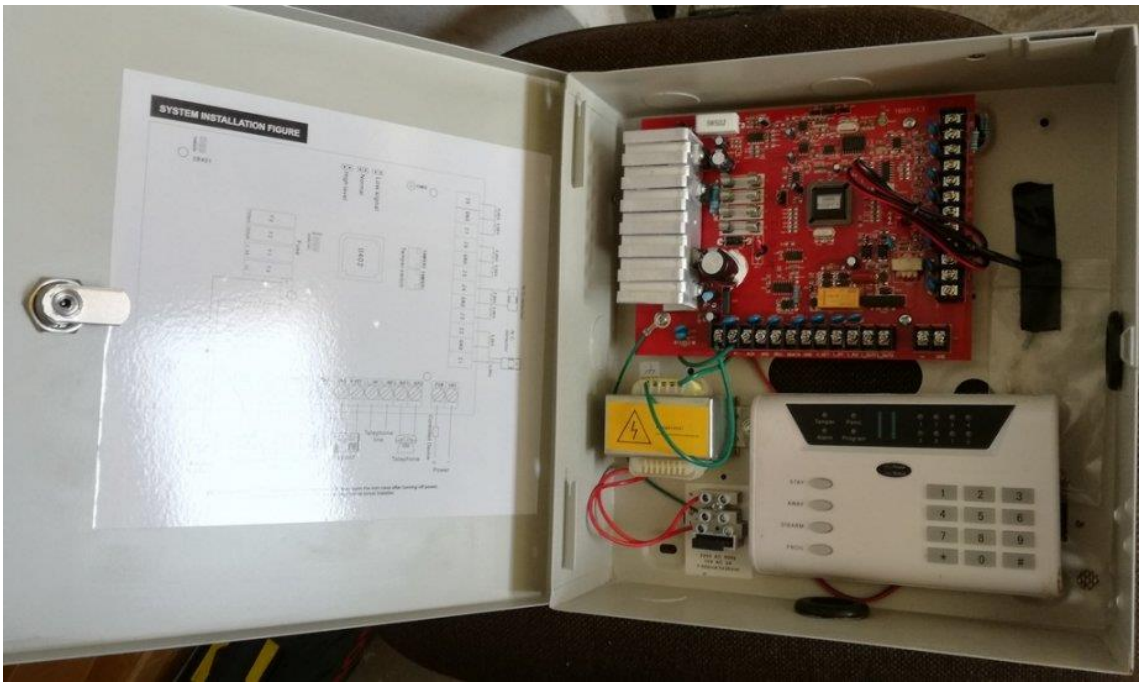
Promjenom stanja kontakata smještenih u detektoru dolazi do pojave razlike napona za normalno stanje, alarmno stanje i sabotažu. Na jedan alarmni ulaz moguće je spojiti više detektora, ali je praktičnije spajati jedan detektor na jedan alarmni ulaz zbog jednoznačnog utvrđivanja detektora koji je izazvao alarm. Time je omogućena brza reakcija u slučaju štetnih aktivnosti na štićeni objekt.

U adresabilnom sustavu detektori se spajaju paralelno u petlje. U jednoj petlji je moguće spojiti više od sto elemenata. Svakom elementu dodjeljena je uloga unutar petlje. Elementi adresabilnog sustava opremljeni su sklopovljem koje im omogućuje konstantnu komunikaciju s centralnim uređajem. Za komunikaciju i napajanje koriste se samo dvije žice. Centralni uređaj slijedno proziva, unaprijed definiranim protokolom, svaki element sustava koji nakon toga dojavljuje svoj trenutni status.

2.9.1. Centralni uređaj - protuprovalna centrala

Element za prijem i obradu alarmnih i svih drugih tehničkih informacija naziva se alarmna centrala. Alarmna centrala je središnji uređaj protuprovalnog sustava. Na alarmnu centralu povezuju se upravljačke tipkovnice, detektori, ulazni i izlazni moduli te sredstva za uzbunjivanje i dojavu. Alarmna centrala konstantno nadzire status svih detektora i ostalih elemanata u sustavu. Prilikom programiranja svakom detektoru dodjeljuje se tip zone. Uobičajeni tipovi zone su standardna, standardna sa zadrškom, 24-satni nadzor, tihi alarm itd. Pri projektiranju sustava bitno je odrediti ukupnu potrošnju svih elemenata sustava, jer u slučaju nestanka mrežnog napajanja sustav se napaja iz baterijskog napajanja koji ima određeno vrijeme napajanja te autonomiju rada. Alarmna centrala mora imati sljedeće karakteristike:
1. autonomno rezervno napajanje
2. mogućnost priključenja više različitih upravljačkih tipkovnica

3. mogućnost korištenja od strane više korisnika s različitim korisničkim šiframa i različitim ovlaštenjima za korištenje sustava, te njihovom registracijom
4. mogućnost priključenja bežičnih ili žičanih proširenja
5. programsku mogućnost podjele sustava u više nezavisnih podsustava
6. zaštitu od neovlaštenog pokušaja otvaranja ili onesposobljavanja sustava i svakog njegovog elementa
7. mogućnost različitih vrsta dojave alrma na više različitih odredišta
8. daljinsko upravljanje i nadzor uz više stupnjeve zaštite podataka



Slika 9. Predodžba alarmne centrale sa tipkovnicom

Prilikom nestanka mrežnog napajanja alarmna centrala mora trenutno nastaviti rad korištenjem rezervnog napajanja (slika 9.) koje ima autonomiju objekta od 8 do 48 sati. Alarmna centrala se može programirati tako da se informacije o nestanku mrežnog napajanja prenesu trenutno ili sa određenim vremenskim kašnjenjem u centralni dojavni sustav. Mogućnost vremenske odgode slanja poruke o nestanku mrežnog napajanja bitna je za situacije kada npr. na većem gradskom području nestane mrežno napajanje. Tada sve alarmne centrale šalju poruku centralnom dojavnom sustav o nestanku mrežnog napajanja i prelaska

na rezervno napajanje, što bi moglo prouzročiti preveliko opterećenje ulaznih linija centralnog dojavnog sustava.

2.9.2. Upravljački paneli – tipkovnica

Za prikaz stanja sustava, upravljanje i podešavanje na centralni uređaj povezuju se tipkovnice. Tipkovnicom se može upravljati dio sustava ili cijeli sustav. Osnovni elementi tipkovnice su numeričke tipke, funkcijske tipke i ekran. U osnovnim izvedbama ekran je zamjenjen LED elementima koji prikazuju trenutni status svakog područja. Više upravljačkih tipkovnica se postavlja na štićenim objektima koji imaju više od jednog ulaza ili više odvojenih upravljačkih mjesta. Postavljanjem upravljačke tipkovnice, operateru je omogućen nadzor i praćanje rada alarmnog sustava. Upravljačkim tipkovnicama (slika 10) može se dodjeliti različiti stupanj nadzora i upravljanja. Svaka upravljačka tipkovnica ima svoju upravljačku adresu, pa se može utvrditi tko, kada i što je radio na kojoj upravljačkoj tipkovnici.

Slika 10. Predodžba upravljačke tipkovnice

Suvremeni centralni uređaji protuprovalnog sustava podržavaju spajanje sa računalom u kojem je program za upravljanje i vizualizaciju sustava. To je korisno u većim objektima sa stalnim dežurstvom, jer omogućuje upravljanje s jednog mjesta, te pregledan grafički prikaz stanja svih elemenata sustava. Operaterima je potreban unos zaporke tj. moraju se identificirati prilikom

pokretanja programa, te se sve operacije operatera pohranjuju. Sustav se može programirati putem računala. Na taj način moguće je preglednije i brže postavljanje parametara sustava nego pri korištenju upravljačke tipkovnice.

2.9.3. Detektori

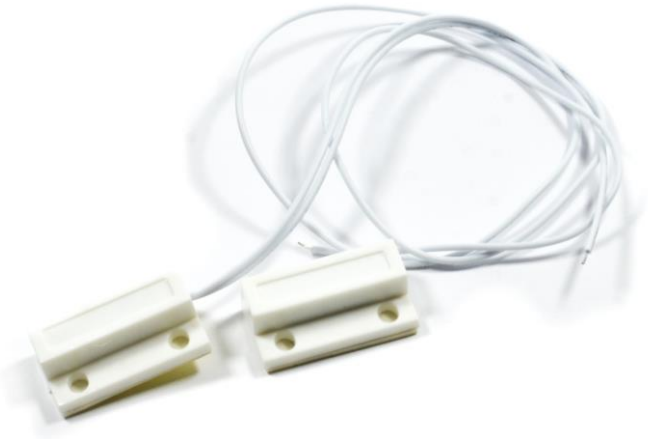
Protuprovalni detektori kao i svi ostali sustavi tehničke zaštite su predviđeni da svako neovlašteno kretanje i djelovanje procesuiraju i na osnovu toga u najkraćem mogućem roku prenesu alarmno stanje na definiranu lokaciju. Prema načinu rada detektore djelimo na:

1. pasivne
2. aktivne

Pasivni detektori funkcioniraju kao prijamnici različitih vrsta signala na osnovu kojih prelaze u alarmno stanje dok aktivni detektori emitiraju signal te ga prihvaćaju i analiziraju. Detektor se najčešće oprema sa dva kontakta. Jedan kontakt služi za kontrolu zatvorenog kućišta, a drugim se dojavljuje nastanak alarma.

1. Magnetski kontakti

Koriste se za detekciju otvaranja vrata ili prozora. Sastoje se od reed releja i magneta. Magnet se postavlja na pokretni dio vrata ili prozora, a reed relej na fiksni. Kada su primaknuti jedan drugom, magnet privlači pokretni dio reed releja u normalno, nealarmno stanje. Kod otvaranja vrata ili prozora, magnet se odmiče od reed releja i gubi kratki se spoj, tada nastaje alarmno stanje. Uglavnom se koriste balansirani magnetski kontakti kako bi se spriječila sabotaža drugim magnetom. Balansirani magnetski kontakti koriste dva magneta, jedan je postavljen na pokretni dio, a drugi na reed relej. U normalnom stanju kontakt je pozicioniran u sredini reed releja, a bilo kakva promjena izaziva alarmno stanje.



Slika 11. Predodžba magnetskih kontakata

2. Pasivni infracrveni detektor- PIR detektor

Pasivni infracrveni detektor je detektor koji u svrhu detekcije pokreta koristi tzv. pasivnu infracrvenu tehnologiju koja omogućuje detekciju isijavanja tjelesne topline. PIR detektori određeni prostor pokrivaju svojim zrakama, te ukoliko se uđe u takvo detekcijsko polje, detektor aktivira alarm. Područje koje detektor pokriva određuje leća koja dijeli zrake, dok u svrhu povećanja pouzdanosti infracrvene detekcije, moderni digitalni detektori pokreta koriste razne algoritme i programirane logike kojima smanjuju mogućnosti lažne aktivacije drugim izvorima topline u prostoru.

Slika 12. Predodžba PIR detektora

Naziv je za tehnologiju koja se koristi u prostorima u kojima postoji rizik od lažnog aktiviranja alarma od strane životinja, bilo da se radi o kućnim ljubimcima ili primjerice o većim skladišnim prostorima se naziva PET immune gdje se ne može spriječiti kretanje miševa, mačaka, itd. Takvi detektori uglavnom primjenjuju tehnologiju koja prepoznaje veličinu životinje, odnosno težinu prema količini isijane topline, i do određene granice primjerice 30 kg ne aktivira alarm. Ukoliko detektira čovjeka, zbog veće količine topline detektor prepoznaje razliku i u tom slučaju aktivira alarm. Kako PIR detektor infracrvene tehnologije reagira na isijavanje topline, postoje određeni uvjeti u kojima isti ne može osigurati kvalitetnu zaštitu bez lažnog aktiviranja, primjerice u prostorijama u kojima postoji plinski bojler, klima uređaji koji su neprestano uključeni, kotlovnice, itd. U takvim otežanim uvjetima rada koriste se dualni detektori koji koriste dvije odvojene tehnologije detekcije, uglavnom standardnu PIR (infracrvenu) tehnologiju i mikrovalove. Kako bi se postigla veća pouzdanost, alarmnom situacijom se smatra tek kada obje tehnologije istovremeno potvrde i kretanje u prostoru i isijavanje topline tijela.

3. Detektori loma stakla

Postoji nekoliko izvedbi detektora loma stakla. Prema mjestu montaže razlikujemo detektore koji se lijepe na štićeno staklo i one koji se postavljaju na zid ili strop u blizini štićenih stakala. Prema načinu detekcije razlikujemo tri vrste detektora:

1. akustični senzori
2. senzori šoka
3. detektori dvostruke tehnologije

Akustični detektori osluškuju i detektiraju visoke frekvencije, tipične za zvuk razbijenog stakla. Takvi detektori opremljeni su procesorom za digitalnu obradu signala i nakon filtriranja i obrade zvučnog signala donose odluku o prelasku u alarmno stanje. Senzori šoka detektiraju frekvenciju 5 kHz koja se emitira pri razbijanju stakla. Kao senzor koristi se piezoelektrični element. Detektori dvostruke tehnologije koriste oba načina detekcije i za prijelaz u alarmno stanje

potrebno je zadovoljiti oba uvjeta. Time je smanjena mogućnost pojavljivanje lažnih alarma.

Slika 13. Predodžba detektora loma stakla

4. Barijere

Koriste se za zaštitu perimetra ili većih unutarnjih prostora. Sastoje se od predajnika i prijamnika. Predajnik konstantno emitira signal koji se u normalnom radu neometano prihvaća na prijamnik. U slučaju izmjenjenog signala ili njegovog izostanka, detektor prelazi u alarmno stanje. Prema principu detekcije razlikuju se:

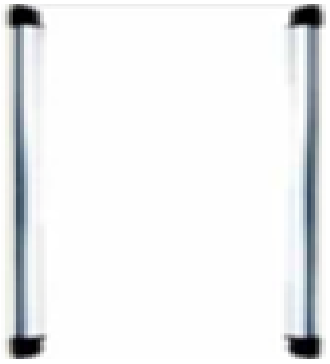
1. Infracrvene barijere
2. Mikrovalne barijere

Infracrvene barijere emitiraju više precizno usmjerenih, moduliranih signala u infracrvenom području. Prolaskom između predajnika i prijamnika prekida se dio infracrvenih zraka i aktivira alarmno stanje. Zaštićeni su od sabotaže modulacijom signala koja bi se promjenila u slučaju pokušaja nadomještaja signala iz drugog izvora. Nedostatak infracrvenih barijera je smanjanje razine signala u uvjetima kiše, magle i sl.

Prijamnik i predajnik mikrovalne barijere mogu se smjestiti u zajedničko kućište ili odvojeno čime se postiže veća udaljenost. Odabirom antene određuje se oblik površine koja se pokriva. Mikrovalne barijere zahtjevaju konstantno

održavanje vanjskog prostora, jer micanje trave, žbunja i sl. uslijed vjetra aktivira alarmno stanje.

.



Slika 14. Predodžba infracrvene barijere

5. Detektor šuma i vibracije

Koriste se za zaštitu trezora, kasa, bankomata i ostalih uređeja i objekata kod kojih se želi detektirati pokušaj mehaničke provale bušenjem, udaranjrm, eksplozijom, itd. Pokušaj provale detektiraju obradom zvuka, poput tetektora loma stakla ili takvom mehaničkom izvedbom detektora da u slučaju vibracije nastaje kontakt i aktivira se alarmno stanje.

Slika 15. Predodžba detektora šuma

2.9.4. Uređaji za uzbunjivanje i dojavu

Nakon pojave alarmnog stanja na jednom od alarmnih ulaza, centralni uređaj prema određenim parametrima, pokreće izlazne uređaje koje čine sljedeći elementi:

- sirena
- bljeskalica
- digitalni i dojavni govornik

1. Sirena

Sirene se djele na unutarnje i vanjske. Unutarnja sirena se smješta unutar štićenog objekta na mjesto gdje nije lako uočijiva i dohvatljiva. Osnovna namjena unutarnje sirene je odvraćanje provalnika od provalničke aktivnosti i uzbunjivanje osoba u većim objektima. Jačina zvuka proizvedena unutarnjom sirenom je veča od 100 db mjerena na udaljenosti 1 m od sirene. Unutarnju sirenu napaja i s njom upravija centralni uređaj.

Za razliku od unutarnje sirene, vanjska sirena postavlja se tako da je uočljiva kako bi ukazala na postojanje alarmnog sustava čime se odvraća provalnička aktivnost. Pozicija ugradnje treba biti odabrana tako da sirena nije lako dohvatljiva. Sirena je zaštićena dvostrukim plastičnim ili metalnim kućištem. Izvedba kućišta omogućuje rad u vanjskim uvjetima i onemogućuje lako skidanje sirene sa zida. Uz nadziranje zatvorenosti kućišta, na stražnjem dijelu kućišta nadzire se pričvršćenost na montažnu površinu. Sirena za napajanje koristi akumulator smješten u zajedničkom kućištu koji se neprekidno napaja i kontrolira iz centralnog uređaja. U slučaju otvaranja kućišta, skidanja sirene i presjecanje žica između sirene centralnog uređaja, sustav prelazi u alarmno stanje, a sirena se automatski uključuje napajajući se iz vlastitog akumulatora. Uz vanjsku sirenu se često u isto kućište ugrađuje i bijeskalica.

Slika 16. Predodžba sirene sa vanjskom bljeskalicom

2. Bljeskalice

Služe za vizualnu identifikaciju sustava protuprovale. Često se postavljaju uz sirene što dodatno olakšava identifikaciju objekta u alarmu, što je korisno ako više objekata u blizini ima ugrađen sustav protuprovale.

3. Dojavnici

a) digitalni dojavnik

Koristi se za dojavu svih događanja u sustavu dojavnom centru unaprijed definiranim formatom poruke. Poruke se šalju u digitalnom obliku pa je prijenos poruka vremenski kratak. Digitalnim dojavnikom dojavljuju se:

- početak i prekid alarmnog stanja uključujući točnu identifikaciju zone koja je izazvala alarm
- početek i prekid sabotaže detektora ili drugih elemenata sustava
- uključenje i isključenje s identifikacijom korisnika
- nestanak i povrat mrežnog napajanja
- periodički test alarmne centrale
- parametriranje sustava

b) Govorni dojavnik

U slučaju da se želi primiti informacija o uključenju alarmnog stanja sustava protuprovale na standardan telefon ili mobitel u obliku govorne poruke koristi se govorni dojavnik. Kada se aktivira alarm, alarmna centrala govorni dojavnik koji

naziva unaprijed programirane telefonske brojeve i započinje reprodukciju jedne od snimljenih poruka, ovisno o događaju. Nedostatak govornog dojavnika je nemogućnost slanja informacija koji detektor je izazvao alarmno stanje.

Slika 17. Predodžba digitalnog dojavnika

2.10. Sustav videonadzora

Sustavi video nadzora baziraju se na primjeni videokamere. Video signal iz kamere vodi do uređaja u nadzornom centru koji omogućuje obradu, prikaz i pohranjivanje slike u digitalnom ili analognom obliku. Osnovne grupe elemenata video nadzora su:

- periferna oprema
- oprema u nadzornom centru

Periferna oprema sustava video nadzora su uređaji za generiranje slike tj. kamere te njena oprema (objektivi, kućišta, pretvorenici signala, reflektori i dr.) koja omogućuje rad kamera i prijenos video signala u zadanim uvjetima. Oprema u nadzornom centru služi za prihvat, distribuciju, obradu i snimanje slika, upravljanje sustavom videonadzora i izmjenu informacija sa trećim sustavima.

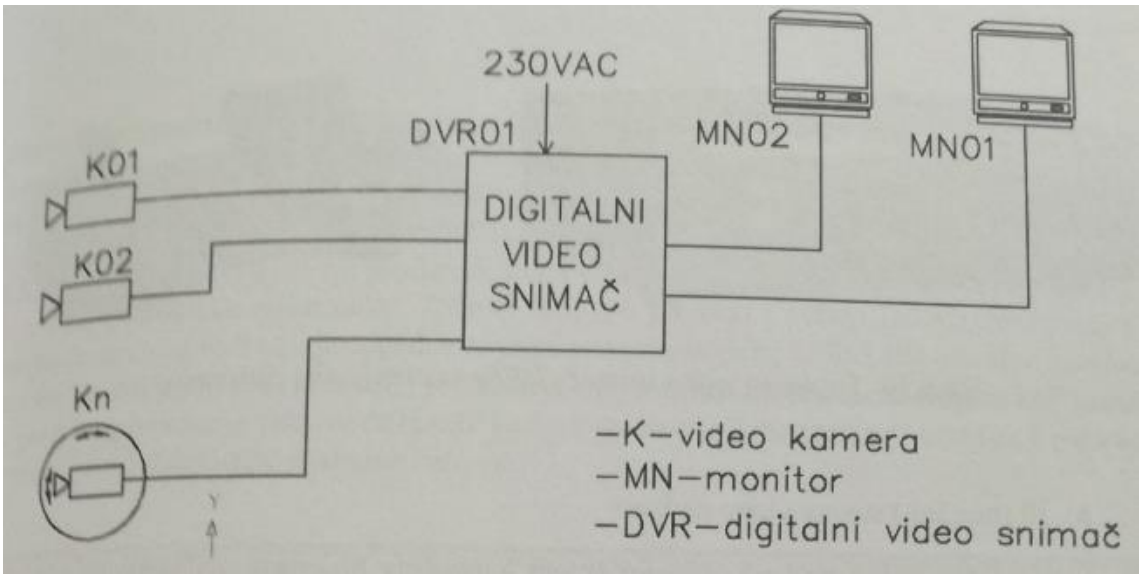
Postoje dvije vrste sustava video nadzora:

- analogni sustavi video nadzora
- IP (mrežni) sustavi video nadzora

a) analogni sustav video nadzora

Sastoji se od:

- videokamere
- opreme za prijenos video signala (kabeli, video pojačala, pretvorenici signala)
- uređaja za obradu i snimanje video signala (preklopnik, matrica,quad, digitalni multipleksre i snimač)
- uređaje za upravljanje kamerama (upravljačka tipkovnica)



Slika 18. Predodžba analognog sustava video nadzora

Sustav može biti baziran na digitalnom snimanju. Slike s kamera snimaju se u digitalnom snimaču koji je ujedno najčešće i multiplekser. Slike se digitalnom formatu pohranjuju na čvrsti disk digitalnog snimača, gdje se automatski kreira baza podataka, te je slikama moguće pristupiti brže, primjenom kriterija pretraživanja (vrijeme, broj kamere). Rezolucija snimljene slike može biti jednaka ili veća u odnosu na video sustav s analognim snimanjem. Rezolucija snimljene slike ograničena je prvenstveno rezolucijom video kamere, te formatom i faktorom kompresije. Primjenom određenog formata kompresije (MPEG, JPEG...), postiže se sažimanje slika s manjim ili većim utjecajem na kvalitetu. Slike se potrebi pohranjuju i na vanjske nositelje podataka kao što su

DAT trake, CD ROM, DVD i sl. Digitalni video multiplekseri (rekorderi) često imaju i mogućnost automatske detekcije aktivnosti. To je funkcija kojom uređaj prati promjene slike s kamera, te ukoliko promjena na slici zadovolji zadani kriterij, aktivira snimanje ili neku drugu akciju. Ovim se načinom dodatno može racionalizirati korištenje kapaciteta diska za snimanje.

b) IP (mrežni) sustav video nadzora

Razvojem informatičkih sustava te povećanjem kapaciteta prijenosa podataka računalnim mrežama omogućen je i prijenos video slika putem računalne mreže. Kod IP sustava većina nadzora slika se prenosi putem TCP/IP protokola unutar LAN mreže mreže ili putem interneta. IP sustavi video nadzora se sastoje od:

- video kamere s video serverom (IP kamera),
- računalne LAN mreže
- osobnih računala s programskom podrškom za nadzor, snimanje i upravijanje.

Slika koja se generira u kameri LAN mrežom se distribuira korisnicima, koji u skladu svojim ovlaštenjima mogu pregledavati, ispisivati zapise ili upravljati kamerama. U takvim sustavima mogu se koristiti analogne ili IP kamere. IP kamere imaju ugrađen mrežni priključak, a analogne kamere se na LAN mrežu priključuju preko video enkodera. Prednost ovakvog sustava je mogućnost uvida u slike kamera s bilo kojeg mjesta povezanog putem računalne mreže.

Glavna prednost IP sustava video nadzora je mogućnost stvaranja slike veće rezolucije od analognih kamera. Veća rezolucija kamere omogućuje nadzor većeg područja uz istu rezoluciju slike ili se isto područje nadzire sa višestrukom većom rezolucijom što omogućuje kvalitetniji zapis i više detalja na slici i snimci.

Tab. 2. Način prijenosa video signala

Način prijenosa	**Potrebni dodatni elementi**	**Tipično mjesto primjene**	**Maksimalna udaljenost**
Koaksijalnim kabelom		Video nadzor prostora unutar zgrade	500 m
Paričnim kabelom	Predajnik i predajnik za parični kabel	Za udaljenost veće od 500 m, tamo gdje je položen parični kabel	1000 m
Bežičnim putem	Bežični predajnik i bežični prijamnik	Na mjestima gdje nije moguće ili je skupo položiti instalaciju	30000 m Tipično do 3000 m
Mikrovalni			
rf			
Optičkim kabelom	Optički predajnik i optički prijamnik	Za vanjske instalacije, za veću udaljenost	10000 m
Informatičkim mrežama	Konverter za priključak		Nije ograničeno

Integracija videa sa sustavom protuprovale i vanjske zaštite omogućuje videoverifikaciju signala alarma što smanjuje troškove za zaštitarske intervencije, a integracija s kontrolom pristupa olakšava svakodnevno poslovanje u objektima koji se štite s više sustava tehničke zaštite. Sustavi videonadzora često se integriraju s drugim sustavima zaštite čime se povećava efikasnost samog sustava, ali i temeljnog poslovanja pojedine tvrtke. Integracija je moguća na razini alarmnih ulaza/izlaza, serijske komunikacije (s POS uređajima, bankomatima) ili na razini programske integracije tj. zajedničkog upravljanja s više sustava što uključuje i videonadzor. Razvoj video detekcije pokreta započeo je s tzv. rasterskom analizom slike. Kod ovog načina rada slika se dijeli na niz pravokutnika za koje se definira jesu aktivni ne, odnosno je li promjena u tom dijelu slike može izazvati alarm. Na ovoj vrsti detekcije zasniva se princip rada detekcije aktivnosti koji je ugrađen u većinu suvremenih

digitalnih video snimača. Za razliku od detekcije aktivnosti uređaj za detekciju pokreta mora imati mogućnost automatskog razlikovanja nedozvoljenog kretanja s minimalnim brojem lažnih alarma. Sofisticirani sustav video detekcije pokreta prema podešenim parametrima programa vrši alarmiranje i upravljanje trećim sustavom.

Alarmno stanje se određuje prema sljedećim kriterijima:

- smjer kretanja
- mjesto kretanja
- minimaina i maksimalna brzina kretanja
- perspektiva (3D detekcija)
- veličina i oblik objekta koji se kreće
- progamska podrška sustava video detekcije pokreta podržava
- parametriranje sustava
- grafičko sučelje za vizualizaciju stanja sustava i upravljanja
- bazu podataka o stanju sustava s napomenama nadzorne osobe

Sustavi video detekcije pokreta koriste se često kao sustavi za zaštitu perimetra visokougroženih objekata kao što su zatvori, aerodromi i sl.

2.11. Protuprepadni sustav

Iako se protuprepadni sustav u većini proizvodnih tvrtki ne koristi, ukratko će biti opisane najbitnije stvari koje je korisno znati. Postavlja se pitanje: zašto se ne koristi protuprepadni sustav u proizvodnim tvrtkama? Odgovor je jednostavan, premali je rizik od protuprepadnog napada na zaštitare ili zaposlanike proizvodne tvrtke pa time i same tvrtke ne žele ulagati i koristiti ovu vrstu zaštite. Najugroženije su novčarske institucije, banke, zlatarne i slične poslovnice koje rade sa vrlo vrijednim artiklima ili direktno sa novcem te da bi osigurale svoju sigurnost, moraju koristiti ovu vrstu zaštite. Proizvodne tvrtke uglavnom ne proizvode toliko vrijednu, tj. dovoljno vrijednu robu (osim tvornice oružja) koje izazivaju pljačkaše na teže kriminalno djelo. Ova vrsta zaštite se razlikuje od protuprovalnog i vatrodojavnog sustava po tome što u navedenim sustavima prelazak iz normalnog u alarmno stanje aktivira na štićenom objektu

svjetlosnu ili zvučnu signalizaciju, dok kod protuprepadnog sustava se aktivira tihi alarm tj. tihu dojavu bez aktiviranja zvučne ili svjetlosne signalizacije i istodobno prijenos alarmne informacije u centralni dojavni sustav (slika 19).

Slika 19. Predodžba centralnog dojavnog sustava

Elementi protuprepadnog sustava su:

- elementi koji služe za označavanje izvan i unutar zaštićenog prostora
- ručna i bežična protuprepadna tipkala (slika 20.)
- nožne alarmne šine
- detektori zadnje novčanice
- elektroničke kase i sefovi sa ugrađenim vremenskim kašnjenjem
- nagazni tepisi
- blindirana dvostruka vrata
- ručni i prolazni detektori metala
- sustavi video nadzora sa pokretnim kamerama
- mjere i postupci tjelesne zaštite koji se poduzimaju na štićenom objektu
- edukacija zaposlenika i klijenata - korisnika usluge banke ili neke druge institucije

Slika 20. Predodžba bežičnog protuprepadnog tipkala

U zemljama gdje prijeti opasnost od terorističkog napada povećan je rizik i napada na velike tvornice. Tako smo imali slučaj prije tri godine kada je Francuskoj u jednoj tvornici izveden teroristički napad sa smrtnim posljedicama. No i sa tim događajem još uvijek je rizik mali da bi se koristio protuprepadni sustav u proizvodnim tvrtkama. Sustavi protuprepadne zaštite se trebaju promatrati isključivo kao dio integralnog sustava zaštite, a najučikovitija metoda za smanjenje ugrožavanja je prventivno djelovanje pomoću instaliranih sustava tehničke zaštite, poduzetih mjera tjelesne zaštite i stalne edukacije zaposlenike i korisnika usluge određene tvrtke.

2.12. Vatrodojavni sustav

Vatrodojavni sustav je sustav koji služi za otkrivanje i dojavu požara u njegovoj najranijoj fazi te uzbunjivanje ljudi i upravljanje pridodanim sustavima koji mogu smanjiti štetne posljedice požara npr. sustav gašenje plinom, sustav ventilacije i klimatizacije, kupole za odimljavanje i sl. Primjenjuje se u prostorima i građevinama gdje je procjenjena ugroženost od požara ili ako posebni propisi zahtijevaju primjenu sustava vatrodojave.

Sustavi za dojavu požara rade na način da se požani alarmi i smetnje javljača požara te ostale smetnje u sustavu induciraju u centrali sustava za dojavu požara i na osnovu njih se poduzimaju određene izvršne radnje (npr. aktiviranje uređaja za uzbunjivanje, aktiviranje uređaja za prosljeđivanje dojave požara i dr.).

Osnovne funkcije sustava za dojavu požara su:

- primanje dojave požara i smetnji od dojavnih elemenata (jednog ili više javljača požara)
- nadziranje glavnih vodova kako bi se pravovremeno uočila neispravnost sustava
- prikazivanje pogonskih stanja sustava

Ostale funkcije sustava:

- uključivanje uređaja za uzbunjivanje
- upravljanje sustavima za zaštitu od požara
- primanje dojava s drugih sustava
- privremeno isključivanje pojedinih djelova sustava
- priključenje dodatnog pokaznog ili upravljačkog uređaja

Prema načinu rada razlikujemo konvencionalne i adresabilne sustave. Konvencionalni sustavi se temelje na zonskoj topologiji, nema povratne linije s posljednjeg javljača prema centrali. Nije moguće vidjeti točnu adresu javljača koji je izazvao alarm već samo zonu u kojoj je alarm nastao. Pojavljuju se u kombinaciji sa sustavom protuprovale. Kabel s kojim se povezuju javljači mora biti od negorivog materijala i crvene boje ili sa crvenim oznakama. Automatski i ručni javljači nesmiju se nalaziti u istoj zoni. Moguće je maksimalno povezat 32 automatska i 10 ručnih javljača u jednu zonu. Pogodni su za izvedbu malih do srednjih sustava za dojavu požara, jer nude pouzdanu detekciju požara i dobar odnos cijene i kvalitete.

Slika 21. Predodžba ručnog javljača požara

Kod adresabilnih sustava javljači požara su povezani u petlju, što omogućava bolju pouzdanost sustava, jer je moguć jednostruki prekid ili kratki spoj petlje, a da svi javljači i dalje normalno rade pod uvjetom da svaki javljač ima izolator petlje. Svaki se javljač na centrali identificira svojom adresom i proslijeđuje izmjerenu analognu vrijednost požarne veličine ili svoje stanje u digitalnom obliku. Na adresabilnu petlju moguće je spojiti druge elemente kao što su uzlazno/izlazni moduli i sirene. Postoje centralizirani i decentralizirani adresabilni sustavi. Centralizirani sustavi rade na način da javljači svoje mjerene veličine prosljeđuju centrali koja obrađuje primljene podatke i odlučuje da li se dogodilo alarmno stanje. Za takav sustav potrebna je snažna centrala i brza koja je u stanju obraditi veliku količinu podataka. Decentralizirani sustavi koriste napredniju tehnologiju i procesore sa javljačima što omogućava analizu podataka mjerenih veličina odmah u samom javljaču. Javljači u tom slučaju prosljeđuju centrali informaciju o svom stanju kao predalarm, alarm, greška i sl. Decentralizirani sustav omogućuje primjenu naprednih algoritama i filtera kako bi se postigla što kvalitetnija detekcija požarnih veličina. Adresabilni sustavi pojavili su se nakon konvencionalnih sustava i tehnološki su napredniji od njih. Pogodni su za sustave srednih veličina i velike sustave do nekliko tisuća javljača požara, jer nude ispis točnog mjesta požara kao i povezivanje sa dodatnim upravljačkim tipkovnicama i računalnim radnim stanicama te je omogućeno povezivanje više centrala.

Elementi sustava vatrodojave su:

- centrala za dojavu požara
- uređaji za signalizaciju, upravljanje i vizualizaciju
- javljači požara
- uzlazno/izlazni moduli
- uređaji za dojavu i uzbunjivanje

Centrale za dojavu požara djelimo na:

- konvencionalne centrale vatrodojavnog sustava koje mogu prihvatiti samo konvencionalne javljače požara
- adresabilne centrale (slika 22.) vatrodojavnog sustava sa predodređenim brojem petlji
- modularne adresabilne centrale vatrodojavnog sustava za velike sustave gdje je moguće proizvoljno odabrati i ugraditi kartice za konvencionalne zone, adresabilne petlje i razna druga komunikacijska sučelja.

Slika 22. Predodžba adresabilna vatrodojavne centrale

Uređaji za signalizaciju, upravljanje i vizualizaciju se koristi kako bi s mjesta različitog od lokacije centrale mogli vršiti nadzor ili upravljanje sustavom za dojavu požara. Kada je potreban samo prikaz stanja sustava za dojavu požara na više lokacija koriste se signalni paneli s LED diodama i tipkovnice s LCD zaslonom bez mogućnosti upravljanja sustavom.

Javljači požara služe da detektiraju požar u prostoru koji nadziru. Djele se na ručne i automatske javljače požara. Najčešće korištene vrste javljača požara su uz ručne, optički i termički javljači požara. Odabir javljača ovisi o požarnim veličinama koje se očekuju u nadziranom prostoru.

Ulazno, izlazni ili kombinirani moduli se koriste za interakciju vatrodojavnog sustava sa trećim sustavom. Ulazni modul prihvaća signale od drugih sustava, a pomoću njih se mogu u vatrodojavni sustav implementirati i nake druge funkcije npr. SOS poziv iz hotelske sobe. Izlazni moduli koriste se za upravljanje drugim sustavima koji moraju odraditi određenu radnju u slučaju požara npr. zatvaranje protupožarnih zaklopki. Kombinirani moduli se koriste gdje je potrebno dobiti potvrdu odrade pojedine upravljačke funkcije npr. zatvaranje vrata sa potvrdom zatvorenosti. Uređaji koji se koriste za dojavu i uzbunjivanje su sirene (samo napajajuće, nadzirane, adresabilne), bljeskalice, razglasi i dojavnici (glasovni, GSM, digitalni).

2.13. Sustavi kontrole pristupa

Osnovna namjena sustava kontrole pristupa je odrediti i kontrolirati tko ima pravo pristupa određenom objektu koji se štiti ili pravo ulaska u štićeni prostor u određenom vremenskom periodu. Uz osnovnu funkciju kontroliranja pristupa, sustavi kontrole pristupa koriste se i za nadzor i upravljanje vratima, a često se koriste za nadzor i upravljanje drugim sustavima u objektu (dizala, rasvjeta, sustav video nadzora, protuprovale, vatrodojave itd.) Osnovne prednosti u odnosu na kontroliranje ulaska mehaničkim ključem su:

- individualno pridjeljivanje prava pristupa
- vremensko ograničenje prava pristupa,
- trajno spremanje informacija o prolasku i ostalim događajima
- lociranje osoba u realnom vremenu
- manji troškovi pri gubitku kartice u odnosu na gubitak ključa

Postoje različiti načini rada i metode identifikacije, a to su:

a) Fizičko posjedovanje:

- ključ
- magnetske kartice
- bar kod
- induktivne kartice
- beskontaktne kartice
- smart kartice

b) Na znanje:
- unos pina
- unos riječi

c) Biometrija:
- otisak prsta
- geometrija šake
- glas
- geometrija lica
- šarenica

Osnovni elementi sustava kontrole pristupa su medij za identifikaciju, čitači, kontroleri upravljačko računalo s programskom podrškom.

Kontrolor (slika 23.) služi za upravljanje radom čitača, pohranu transkacija, upravljanje električnim bravama i drugim elementima zaprečavanja pristupa, nadzor vrata i komunikaciju s računalom. Opremljen je programabilnim digitalnim ulazima, relejnim izlazima i sučeljem za komunikaciju sa čitačima i računalom. Napredne mogućnosti kontrole su potpuni nadzor kretanja osoba po prostorima, primjena zabrane ponovnog prolaska ograničavanje broja osoba u prostoriji, itd.

Slika 23. Predodžba kontrolora

Čitači se najčešće spajaju sa kontrolorom kojem prenosi informaciju o indetifikaciji korisnika. Čitač je opremljen elementima za svjetlosnu i zvučnu signalizaciju rada i dozvoljenog i nedozvoljenog pristupa. Može biti opremljen relejnim izlazom za prosljeđivanje alarma sabotaže i relejnim izlazom za lokalnu kontrolu vrata. Neki čitači su opremljeni procesorom i memorijom koja im omogućuje samostalnu provjeru određenog broja kartica, PIN-a ili biometrijskih podataka u slučaju prekinute komunikacije sa kontrolorom. Čitači mogu biti:

- čitači s unosom pina
- magnetski čitači
- beskontaktni čitači
- biometrijski čitači

Programska podrška koristi se za parametriranje, nadzor i upravljanje sustavima, te komunikacijom s elementima sustava. Osnovna funkcija programske podrške je definiranje profila pristupa kojima je određeno u kojem periodu se dozvoljava pristup određenom objektu i njihovo pridjeljivanje svakoj osobi u sustavu. Programska podrška omogućuje prikaz događaja vezanih uz kontrolu prolaska, alarmnih situacija i dogadaja važnih za rad sustava u realnom vremenu te izradu različitih izvještaja. Grafička aplikacija omogućuje manipulaciju sustava putem grafičkog sučelja. Na sučelju su prikazani tlocrti štićenih prostora i u njima raspoređeni elementi sustava kontrole (računala,

kontroleri, čitači, vrata) te elementi drugih sustava. Na grafičkom prikazu prikazano je trenutno stanje vrata (otvorena, zatvorena, blokirana itd.) i elemenata drugih sustava. U slučaju pojave alarma automatski se na ekranu prikazuje crtež prostora u kojem nastaje alarm. Prihvat i potvrdu alarma moguće je izvršiti u samoj aplikaciji. Isto tako, moguće je odmah poduzeti potrebne korake (aktiviranje glavnog alarma, deblokada vrata i sl.).

2.14. Tjelesna zaštita

Poslove tjelesne zaštite obavljaju licencirani (sukladno odredbama Zakona o privatnoj zaštiti), moderno opremljeni, a po potrebi i naoružani zaštitari, odjeveni u službene odore ili odjela, koji štite osobe i imovinu te su spremni obavljati i ostale poslove, kao što su prijem stranaka, rad na telefonskoj centrali i sl. Prema odredbama Zakona o privatnoj zaštiti, ovlasti osoba kojima je izdano dopuštenje za obavljanje poslova tjelesne zaštite, dakle čuvara i zaštitara su:

1. provjera identiteta osoba
2. davanje upozorenja i zapovjedi
3. privremeno ograničenje slobode kretanja
4. pregled osoba, predmeta i prometnih sredstava
5. osiguranje mjesta događaja
6. uporaba zaštitarskog psa
7. uporaba tjelesne snage
8. uporaba vatrenog oružja

Od nabrojanih ovlasti, čuvari ne mogu koristiti ovlasti pod točkom 6., 7., i 8.

Tijekom obavljanja poslova tjelesne zaštite, kada su ispunjeni zakonski uvjeti čuvari i zaštitari svoje ovlasti mogu primijeniti:

- unutar štićenog objekta i oko štićene osobe do granice prostora za čije su zaduženi
- na javnoj površini samo temeljem posebnog odobrenja koje izdaje nadležna policijska uprava na prijedlog jedinica lokalne samouprave
- zaštitar kod obavljanja poslova neposredne tjelesne zaštite samo radi odbijanja istodobnog ili izravno predstojećeg napada usmjerenog prema njemu ili osobama koje štiti. U neposrednoj primjeni danih ovlasti čuvari i zaštitari

nikada ne smiju gubiti iz vida terneljina prava i slobodu čovjeka. To znači da su kod primjene ovlasti dužni imati u vidu sljedeće:
- čovječnost - u svakom postupanju poštivati poštivati dostojanstvo, čast i ugled svake osobe te druga temeljna prava i slobode čovjeka
- razmjernost - primjenjena ovlast ne smije izazvati veće štetne posljedice od onih koje bi nastupile da čuvar ili zaštitar nije primjenio ovlasti.

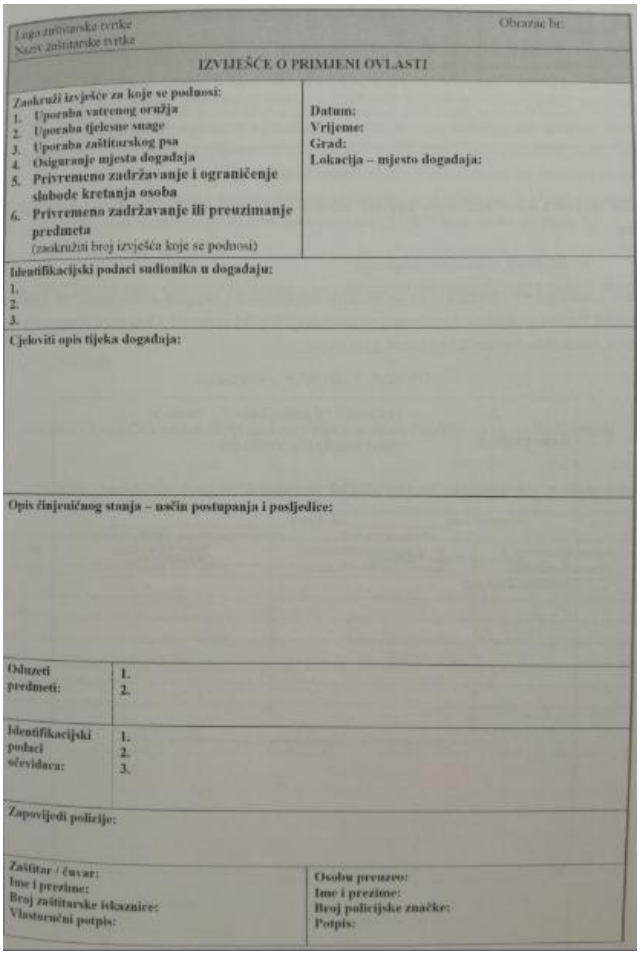
Čuvari i zaštitari tijekom obvljanja tjelesne zaštite mogu provjeriti identitet osobe:
1. prilikom ulaska i izlaska iz štićenog prostora ili objekta
2. koja se zatekne u prijevoznom sredstvu pri ulasku i izlasku iz štićenog prostora ili objekta
3. koja se zatekne u prostoru na kojem je privremeno ograničena sloboda kretanja
4. koja se zatekne u izvršenju prekršaja ili kaznenog djela
5. po zapovjedi policijskog službenika

Upozorenja i zapovjedi izdaju se usmeno, što je i najčešći oblik tijekom obavljanja tjelesne zaštite, pismeno što je praksa pokazala da određivanje nekog pravila u pisanom ili slikovitom obliku ima veliki preventivni značaj. Ovakav oblik ponašanja ističe se boljom razumljivošću, pojačava pedagoški učinak, osnažuje pravilo i podiže etički prag koji prekršitelj mora prijeći, te pokretima ruku, uglavnom za ograničenje slobode kretanja. Upozorenja i zapovjedi moraju biti zakonita, kratka, jasna i precizna, razumljiva i izvediva koja se mogu izdati fizičkoj osobi i odgovornoj osobi u pravnoj osobi. Čuvari ili zaštitari mogu koristiti ovlast privremenog ograničenja slobode kretanja u štićenom prostoru ili objektu zbog sprječavanja izvršenja kaznenih djela ili prekršaja, hvatanja odnosno dovođenja pod svoju kontrolu počinitelja kaznenih djela i prekršaja te osiguranje svjedoka i dokaza koji mogu poslužiti u kaznenom ili prekršajnom postupku te po potrebi zadržati osobe.

Slika 24. Predodžba privremenog ograničavanja slobode kretanja

Prema Zakonu o privatnoj zaštiti i pravilniku o uvjetima i načinu provedbe tjelesne zaštite, čuvar i zaštitar su ovlašteni prilikom ulaska i izlaska iz štićenog prostora obaviti pregled osoba, predmeta koje osoba nosi sa sobom i prometnog sredstva.

Zaštitari prema zakonu mogu upotrijebiti tjelesnu snagu ako ne mogu odbiti protupravni i neposredni napad kojim se ugrožava njihov život ili život osoba koje čuvaju ili ako ne mogu odbiti protupravni ili neposredni napad usmjeren na uništenje i smanjivanje vrijednosti imovine, a da pri tom štetne posljedice budu veće od prijetećih. Tjelesnu snagu mogu provoditi radi svladavanja otpora, svladavanje bijega i ako zakonito izdana upozorenja i zapovijedi ne jamče uspjeh. Zaštitar će primjeniti tjelesnu snagu kao zahvat udarac ili neka vještina obrane ili napada kojima se prisiljava osobu na poslušnost uz što manje štetnih posljedica. Svako djelovanje čuvara ili zaštitara treba biti evidentirano dokumentom zvanom Izvješće o primjeni ovlasti (slika 25.).



Logo zaštitarske tvrtke
Naziv zaštitarske tvrtke

Obrazac br:

IZVJEŠĆE O PRIMJENI OVLASTI

Zaokruži izvješće za koje se podnosi:
1. **Uporaba vatrenog oružja**
2. **Uporaba tjelesne snage**
3. **Uporaba zaštitarskog psa**
4. **Osiguranje mjesta događaja**
5. **Privremeno zadržavanje i ograničenje slobode kretanja osoba**
6. **Privremeno zadržavanje ili preuzimanje predmeta**

(zaokružiti broj izvješća koje se podnosi)

Datum:
Vrijeme:
Grad:
Lokacija – mjesto događaja:

Identifikacijski podaci sudionika u događaju:
1.
2.
3.

Cjeloviti opis tijeka događaja:

Opis činjeničnog stanja – način postupanja i posljedice:

Oduzeti predmeti:	1. 2.
Identifikacijski podaci očevidaca:	1. 2. 3.

Zapovijedi policije:

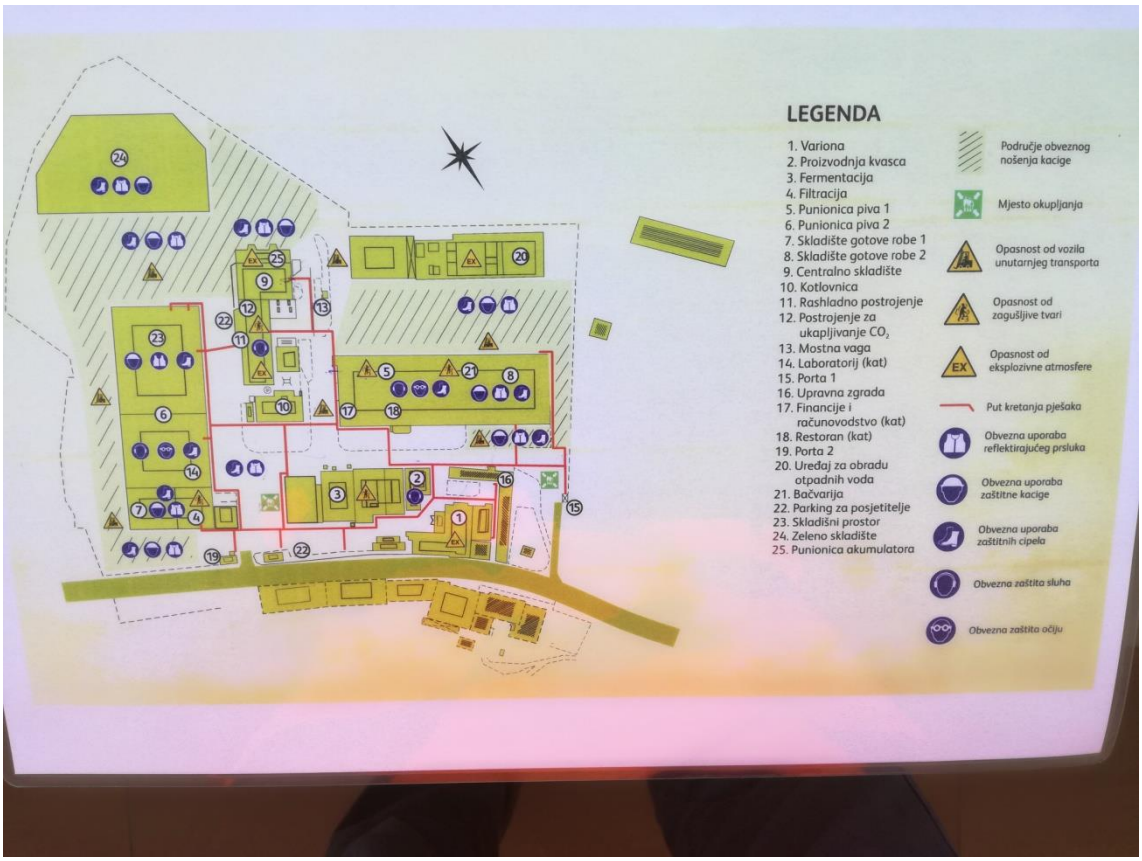
Zaštitar / čuvar: **Ime i prezime:** **Broj zaštitarske iskaznice:** **Vlastoručni potpis:**	**Osoba preuzeo:** **Ime i prezime:** **Broj policijske značke:** **Potpis:**

Slika 25. Predodžba izvješća o primjeni ovlasti

Svrha izvješća je provjeravanje zakonitosti uporabe primjenjene ovlasti čuvara ili zaštitara te omogućuje saznanje o tijeku događaja što može pomoći policiji, ako se radi o nekom slučaju. Sadržaj mora biti jasan i pregledan, izbjegavati poštapalice i kratice koje nisu uobičajene i svakom razumljive. Upotrebljavati stručne izraze. Precizno i točno bilježiti vrijeme svakog događaja. Opis događaja treba biti sažet redoslijedom kako je događaj odvijen. Precizno opisan treba biti način postupanja, vrsta upotrebljavanih sredstva prisile i moguće posljedice.

3. PRAKTIČNI DIO

Praktični dio ovog Završnog rada sastoji se od dobivenih podataka obilaskom, promatranjem i zapažanjem u jednoj proizvodnoj tvrtci.



Slika 26. Predodžba tlocrta proizvodne tvrtke

3.1. Opis proizvodne tvrtke

Predmetna proizvodna tvrtka koja je analizirana u ovom radu bavi se proizvodnjom i distribucijom piva te posluje sa vanjskim izvođačima, uslužnim tvrtkama, tvrtkama kupcima i trgovačkim putnicima kroz nekoliko tipova objekata u pogonu tvrtke. Na tlocrtu proizvodne tvrtke može se vidjeti popis objekata koji se nalaze u krugu tvrtke. Glavna podjela objekata je ta da određeni objekti čine pogonski dio, određeni objekti čine upravni dio te postoje objekti koji čine i pogonski i uredski dio u jednom. Oko objekata sa unutarnje strane nalazi se transportna cesta sa znakovima sukladno prometnim

propisima. Sa vanjske strane je uglavnom žičana ili betonska ograda, a na jednom djelu je zelena površina kojoj je vanjski dio također ograđen žičanom ogradom. Svi pogonski objekti koji imaju naziv po procesu (fermentacija, variona, filtracija, itd...) opremljene su kamerama kojima je primarni zadatak nadziranje strojeva i pogona, a sekundarni praćenje osoblja.

Slika 27. Predodžba kamere za nadziranje procesa

Drugi pogonski objekti su skladišta. U skladištima se ne nalaze kamere i nemaju sustav videonadzora. Zašto je tako? To je tako zato što je kompletna transportna cesta obuhvaćena videonadzorom prema najvišem stupnju zaštite. Svake sumnjive radnje su prepoznatljive prilikom izlaska iz skladišta ukoliko osoba (radnik, vozač, posjetitelj i sl.) pokušaju otuđiti robu. Također, na portama se vrši pregled svih osoba i vozila koje ulaze i izlaze iz samog kruga tvrtke. Svi objekti imaju instaliran vatrodojavni sustav sa prednaponskom zaštitom u obliku kapsule radi zaštite od grmljavinskog vremena. Ukoliko bi došlo do kvara, vatrodojavna centrala bi to prepoznala i javila centrali sa zaštitarima.

Slika 28. Predodžba skladišta

U djelovima objekata gdje se nalaze uredi jedina zaštita je mehanička zaštita, tj. kontrola prolaza beskontaktnim karticama što omogućuje prolaz samo onih osoba koje posjeduju odgovarajuće beskontaktne kartice, a to su zaposlenici. Smatra se da u uredima nema potrebe za videonadzorom, jer radnici nemaju konkurentski odnos (primjerice kao u marketingu) pa se podrazumijeva da je premali rizik za krađu podataka. Svako računalo u uredu je zaštićeno lozinkom koju dobije radnik koji radi za svojim računalom.

Svaki zaposlenik tvrtke koji ulazi i izlazi mora se identificirati beskontaktnom karticom za evidentiranje radnog vremena. Identifikacija je povjerljiva i vidljiva u programu Visual SM. Ostale osobe koje ulaze i izlaze zapisuju zaštitari, također vrši se pregled svih motornih vozila te zapisivanje registracije. U krug tvrtke ulaze kamioni koji dovoze sirovine, vraćenu robu, praznu ambalažu, te sve ostale stvari za potrebe tvrtke. Također kamioni ulaze i za utovar robe. Zaštitari pregledavaju kamione te utovarena roba mora se podudarati sa nalogom kojeg

imaju zaštitari, kako bi se preventivno djelovalo ukoliko se stavi roba u krivi kamion, da se na vrijeme reagira. Proces dobivanja gotove robe je po pogonskim objektima, koji se toči u punioni, a iz punione se smješta u skladište te je spremno da se plasira na tržište.

3.2. Analiza sustava zaštite na svim objektima

3.2.1. Protuprovalni sustav

Protuprovalni sustav na svim objektima baziran je na mikroprocesorskom centralnom uređaju. Takav sustav proširiv je do 128 ulaznih zona detekcije, ima mogućnost telefonske dojave zaštitarima na porti 1, a dodatno je proširiv s LAN i GSM komunikatorom. Centralni uređaj može se programski podijeliti na 8 nezavisnih sektora (particija), sa 16 mogućih mjesta upravljanja pomoću LCD tipkovnica. Uređajem može upravljati do 1000 korisnika, pomoću svojih kodova koji mogu biti četveroznamenkasti ili šesteroznamenkasti. Zone detekcije na ovom centralnom uređaju mogu se izvesti kao nadzirane sa jednim ili dva otpornika ili kao nenadzirane, a svi kablovi do perifernih uređaja zaštićeni su 24 sata od sabotaže. Osim navedenih proširenja moguće je dodati do 8 dodatnih napajanja od 2A za napajanje perifernih uređaja, 16 modula s tranzistorskim izlazima i modulom za bežične detektore. Zaštitari 24 sata nadziru protuprovalnu centralu.

Slika 29. Predodžba šatora

Na objektima u krugu predmetne proizvodne tvrtke ne postoje uređaji za protuprovalnu zaštitu, a planira se postaviti jedan PIR detektor kod robe za izvoz u jednom šatoru (slika 29.). Prema procjeni ugroženosti i sigurnosnom

elaboratu ovlaštene tvrtke, smatra se da je sustav video nadzora koji obuhvaća sve objekte i sav transportni put te pregled zaštitara na izlazu iz tvrtke dovoljan za sprječavanje krađe. No ipak se na navedeno mjesto planira postaviti PIR detektor na baterije, jer je to mjesto najslabije vidljivo na monitoru kojeg snima dotična kamera. Zato će uz PIR detektor postaviti i kameru koja će se aktivirati njegovom reakcijom. To je česta kombinacija za zaštitu od krađa, kamera je u normalnim okolnostima u "stand by" modu, a kada se pojavi osoba, tada PIR detektor detektira promjenu topline te se aktivira što automatski pali kameru koja preko centrale pali monitor te signalizira zaštitarima da obrate pozornost na tu zonu. Time će se pojačati nadzor te zone te će biti vrlo dobro vidljivo tko se nalazi u toj zoni, da li radnik koji obavlja svoj zadatak ili netko tko se sumnjivo ponaša i nosi sa sobom predmet koji nije u skladu sa tim mjestom, primjerice torba, vrećica ili ruksak.

3.2.2. Protuprepadni sustav

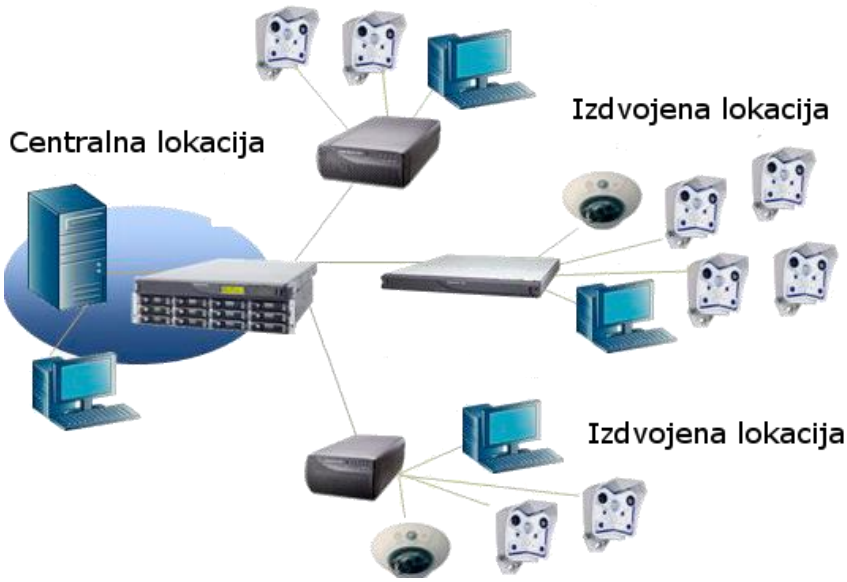
Kao što je ranije navedeno protuprepadni sustav se ne koristi u većini proizvodnih tvrtki, pa tako ni u ovoj. Smatra se da je rizik premali da bi se dogodila ovakva vrsta napada. Na pitanje o protuprepadnom sustavu koje je bilo postavljeno šefu tvrtke koja je zadužena za tehničku i tjelesnu zaštitu odgovor je bio, kao što je navedeno, zbog premalog rizika da se to dogodi, popraćeno sa smješkom (uvjeren da se takav napad neće dogoditi). Što se tiče protuprepadne zaštite, valja spomenuti da je protuprepadna kategorija dio tehničke zaštite koja podrazumijeva razne zabrane u obliku naljepnica (zabranjen ulaz neovlaštenim osobama) i znakova (zabranjen prilaz, slika 30.) te upozorenja (objekt je pod video nadzorom).

Slika 30. Predodžba znaka zabrane prilaza

3.2.3. Sustav video nadzora

Sustav video nadzora temelji se na digitalnom video snimaču koji pohranjuje zapise na tvrdi disk u digitalnom obliku. Uglavnom se koriste analogne video kamere osim u posebnim slučajevima kada je potrebno više detalja za kasniju analizu, tada se koriste megapixelne IP kamere. Bitne značajke digitalnog snimača su:

- detekcija pokreta u slici
- arhiva video zapisa minimalno 30 dana
- minimalno 10 slika u sekundi
- pregled pohranjenog video zapisa na monitoru bez prekidanja pohrane
- izbor više različitih načina prikaza na monitoru (slijedni, više kamera istovremeno)
- spajanje na mrežni sustav i pregled snimača preko WEB sučelja
- vremenska sinkronizacija sa vremenskim serverom
- mogućnost snimanja video zapisa na vanjski medij
- nekoliko video ulaza i izlaza za integraciju sustava
- mogućnost spajanja pokretnih kamera
- mogućnost slanja mail poruke o događajima i statusu snimača



Slika 31. Predodžba sustava videonadzora

Opis rada sustava videonadzora u predmetnoj tvrtci:

Osnovna namjena je zaštita građevina od provala. Sustav je koncipiran da omogućuje nadzor iz jedne porte na cijelu lokaciju. Analogne kamere su povezane koaksijalnim kabelom s videorekorderom. Diditalne kamere su povezane u LAN i wireless mrežnim videorekorderom i nadzornom PC komunikacijskom infrastrukturom na koaksijali. Snimanje na hard diskovima. Pokretnim kamerama upravlja softwer koji omogućuje zaštitaru poduzimanje aktivnosti. Za prikazivanje video slike sa analognog sustava koristi se videorekorder s monitorom. Za prikazivanje video slike sa digitalnog sustava koristi se umreženo PC računalo s monitorom opremljeno programom NUVO. Napajanje sustava je iz opće energetske mreže 230 V, 50 Hz preko UPS-a. Elementi videonadzora:

- centralni uređaj
- kamere s pripadnom opremom
- komunikacijska oprema
- uređaji za prikazivanje
- izvori napajanja električnom energijom
- kabelska instalacija

3.2.4. Sustav kontrole prolaza

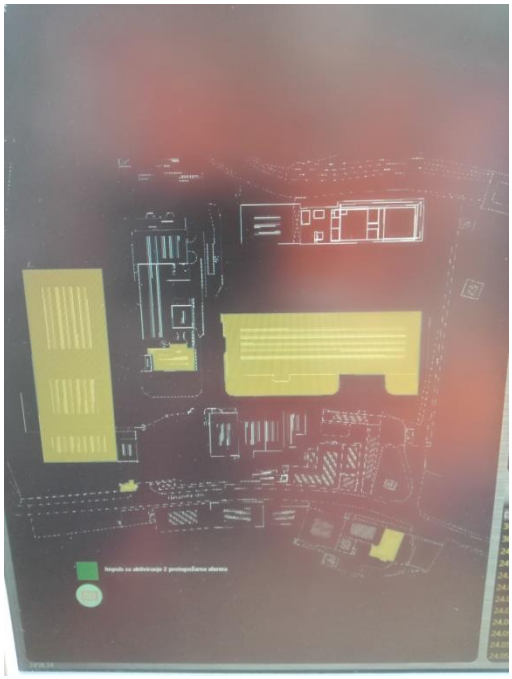
Sustav kontrole prolaza je u kontroli zaštitara. Svaka osoba koja ulazi u krug tvrtke je pregledana i evidentirana od strane zaštitara, osim zaposlenika koji se identificiraju sa beskontaktnom karticom. Identifikacija je vidljiva i povjerljiva u programu Visual SM. Sustav kontrole ulaza izveden je od istog proizvođača na svim objektima u kojima se nalaze uredi, a to su upravna zgrada, financije i računovodstvo i laboratorij. Ovako se mogu uvijek koristiti iste kartice, a sustav je objedinjen u zajedničku bazu podataka s praćenjem na centralnom mjestu. Sustav je koncipiran na kontrolerima razmještenim po objektu. Svaki kontroler može upravljati s dva čitača beskontaktnih kartica (jedna vrata obostrano ili dvoja vrata jednostrano). Kontroleri su povezani UTP kabelom na lokalnu mrežu tehničke zaštite. Aplikacija za upravljanje kontrolerima nalazi se na virtualnim serverima dok je baza izdvojena na database serveru. Svi serveri i baza su u

redovitom procesu backupa. Kontroleri posjeduju autonomno napajanje tako da rade i prilikom nestanka električne energije. Svaki je proširiv s dodatnim relejnim izlazima pa se po potrebi mogu izvesti razne međuovisnosti među pojedinim vratima ili vremensko zatezanje otvaranja vrata. Sustav konstantno prati otvorenost vrata tako da u slučaju nasilnog otvaranja (bez autorizacije karticom) odmah dojavljuje alarmni signal na centralu uz koju je minimalno jedan zaštitar 24 sata dnevno. Isto se događa i kada vrata ostanu otvorena duže nego što je to programski omogućeno. Na vratima koja su predviđena za evakuaciju projektom je predviđeno da se ugradi „fail safe“ elektroprihvatnik koji u slučaju aktivacije vatrodojave ostavlja vrata u otvorenom stanju. Osim ovog, pokraj svakih vrata postavljena je kutija za čuvanje ključa za evakuaciju do kojeg se može doći razbijanjem stakla priloženim čekićem. Kutija za ključ spojena je na protuprovalni sustav i dojavljuje signal razbijanja stakla na centralu.

3.2.5. Vatrodojavni sustav

Vatrodojavni sustav na promatranim objektima koncipiran je na dvije vrste centralnih uređaja. Ovisno o veličini objekta implementirane su ili klasična vatrodojavna centrala ili na većim objektima analogno-adresabilna vatrodojavna centrala. Na svim objektima vatrodojavni sustav izveden je na način da je centrala smještena u porti dva. Svaka vatrodojavna centrala spojena je preko komunikatora u protuprovalnoj centrali na 24 satni tehnički nadzor i to dojava požara i greške vatrodojavne centrale. Na porti jedan postavljen je upravljački LCD display s prikazom statusa vatrodojavne centrale.

Dvije centrale vatrodojavnog sustava nalazi se u porti dva, a sirena na krovu porte 2. U krugu tvornice postavljena su ukupno 5 ručnih i 14 zona s automatskim javljačima požara. Sustav je u potpunosti pod nadležnošću zaštitara. Kod aktiviranja bilo kojeg javljača požara u vrijeme dok je porta dva otvorena, zaštitar obavještava javnu vatrogasnu postrojbu (JVP) na broj 0193 da je aktiviranje primjećeno, no intervenciju ne traži dok ne izvrši provjeru. Provjerava koji je alarm aktiviran te provjerava oznaku na ekranu (slika 32.).



Slika 32. Predodžba praćenja rada vatrodojavnog sustava

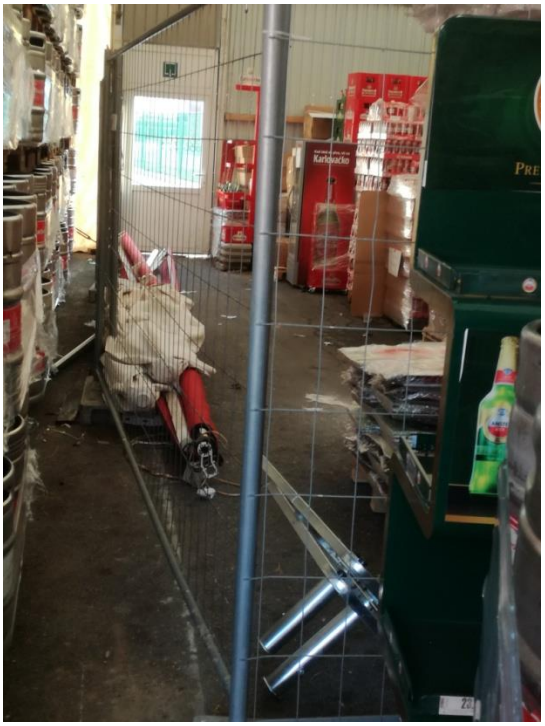
Alarmirajući odgovornu osobu u dijelu tvornice gdje se aktivirao alarm i kolege zaštitare na porti jedan utvrđuje stanje. Ako je alarm bio lažan i došlo je do aktiviranja zbog nekog drugog uzroka (koncentracije pare, nepažnje, vlage), izvještava JVP. Ukoliko je požar stvaran i snagama djelatnika tvornice nije ga moguće ugasiti, poziva JVP na intervenciju. Po završetku svih radnji, vatrodojavnu centralu ponovnu uključuje potiskom na tipku „reset“. Nakon resetiranja kratko sačekati i pratiti stanje centrale, a o djelatnostima izvjestiti JVP. U slučaju stvarnog utvrđivanja početnog požara manjeg intenziteta, zaštitar pristupa gašenju koristeći PP aparate i druga priručna sredstva. Ako je prosudba da se požar ne može ugasiti, zahtjeva se intervencija JVP. Zbog sprečavanja nastanka mogućih većih šteta, sve ove aktivnosti odvijaju se vrlo žurno, ali uz maksimalnu opreznost i pravilne prosudbe. Kod dolaska JVP zaštitari otvaraju glavna ulazna vrata, izvješćuju zapovjednika ekipe o mjestu i intenzitetu požara, pokazuju požarne putove te upoznaju zapovjednika s lokacijom glavne sklopke za električnu mrežu, opasnim materijalima u tom području te rasporedom hidrantske mreže. Tokom gašenja požara, zaštitari pojačavaju nadzor i zaštitu objekta i spriječavaju pristup osobama koje ne

sudjeluju u gašenju požara. Obavezni su o nastaloj situaciji izvjestiti MUP, odgovorne osobe same tvrtke i tvrtke pružatelja tjelesne i tehničke zaštite, a ako je alarm bio lažan napisati izvješće. Vatrodojavna centrala može detektirati greške u sustavu. Kao i kod aktiviranja alarma, centralu utišati. Nakon određenog vremena resetirati te po potrebi ponoviti postupak. Ponavlja li se greška, ostaviti utišano i izvjestiti ovlaštenog servisera. Svi vatrodojavni sustavi redovno se održavaju dva puta godišnje, a jednom se izvodi periodički godišnji pregled od ugovorenog ovlaštenog partnera. Svi nalazi s redovnih pregleda upisuju se u knjigu održavanja, a o godišnjem periodičkom ispitivanju ovlaštena tvrtka izdaje uvjerenje o funkcionalnosti sustava.

3.2.6. Sustav mehaničke zaštite

Sustavom mehaničke zaštite smatraju se razne fizičke barijere, rešetke, protuprovalna vrata, protuprovalne brave i sl. Na promatranim objektima uglavnom se postavlja mehanička zaštita najnižeg stupnja, tj. vrata koja je moguće otvoriti s obje strane ili samo s unutrašnje strane objekta. U ranije spomenutim objektima postoji sustav kontrole prolaza pomoću beskontaktnih kartica. Minimum zaštite je i u ostalim objektima kao što su skladišta i šatori sa gotovom robom i proizvodom. Zaštita je uglavnom mehaničkom pregradom ili ogradom, bez uporabe elektroničkih naprava, a prostorije u kojima se nalaze manje stvari poput naljepnica, selotejpa, ljepila i sl. se zaključavaju običnim ključem. Pitamo se zašto je to tako. Razlog je taj da je tvrtka dala svu ovlast zaštitarima i uloga zaštitara je da prate neovlašten ulaz u bilo koji objekt.

Poslodavac podrazumijeva da zaposleni radnici ne kradu gotove proizvode i vlasništvo tvrtke, jer u slučaju otkrivanja dolazi do direktnog otkaza. Ipak, poslodavac ne može imati potpuno povjerenje u radnike niti u zaštitare pa na ovaj način (slika 33.) štite robu i materijale.



Slika 33. Predodžba mehaničke zaštite

Na prikazanoj slici vidimo metalnu ogradu povezanu plastičnom vezicom, te sa strane postavljene palete koje onemogućuju otvaranje same ograde. Nedostatak ovakve zaštite je taj da se ograda može preskočiti i otuđiti bilo koji materijal iz štićenog prostora. Upravo zato zaštitari pregledavaju sve osobe na izlasku iz tvrtke kako bi otkrili bilo koga u pokušaju krađe. U promatranoj tvrtci mehanička zaštita ima najveće značenje za sve osobe i radnike da štićenu robu ili materijale "ne diraju" bez dozvole nadređene osobe.

3.2.7. Tjelesna zaštita

Zakonska obveza je da tvrtka ove veličine i djelatnosti kojom se bavi ima tjelesnu zaštitu. Usluga pružanja tjelesne zaštite, kao i tehničke zaštite ugovorena je sa istom zaštitarskom tvrtkom. Tvrtka ima dvije porte, porta jedan i porta dva. Zaštitari imaju najveće ovlasti za spriječavanje nedozvoljenih radnji i neovlaštenog ulaska i izlaska. Slijedi opis općih i posebnih dužnosti zaštitara u opisanoj proizvodnoj tvrtci:

1) opće dužnosti zaštitara

- zaštitari na radno mjesto dolaze uredni, u psihofizičkom stanju za uspješno obnašanje dužnosti, prema važećem rasporedu rada, a dužnost obnašaju u propisanoj odori, sa vidljivo istaknutom iskaznicom i ažurnim radnim nalogom
- zaštitari na smjenu dolaze 10 minuta prije prijema kako bi se upoznali sa stanjem objekta, radnog mjesta, mogućim promjenama, novim nalozima i zadaćama i izvršili uvid u objekat i prateću dokumentaciju , novoprimljeni nalozi, zadaće ili naputci mogu biti kao dokument u pisanom obliku, zaprimljeni elektroničkom poštom ili preneseni usmeno uz zabilježbu u knjizi obavijesti
- zaštitar obavlja neposrednu tjelesnu zaštitu osoba i imovine putem zaštitarskih poslova i ophodnjom štićenih objekata
- nadzire ulazak i izlazak osoba, roba i vozila iz štićenog objekta, te prema ovlastima i pravilima provjerava identitet osoba, pregledava osobe i prometna sredstva, daje upozorenja i zapovijedi, osigurava mjesto događaja, uporabi tjelesnu snagu, privremeno ograničava slobodu kretanja
- pregled osoba vrši vizualno, uvidom u sadržaj predmeta koji osoba nosi što mu ista mora omogućiti. Prtljažnik vozila ili teretni prostor kamiona radi pregleda otvara isključivo vozač osobno.
- za predmete koje pronađu u osobnoj prtljazi ili prtljažniku vozila, a koji mogu biti imovina tvrtke i mogući predmet otuđenje ili neodobrenog iznošenja, od osobe zatražuju porijeklo dobave predmeta, provjerava sa odgovornim osobama tvrtke. Ne dozvoljava izlazak do završetka postupka utvrđivanja stanja.
- predmete koje pronađu prilikom pregleda, a koji mogu biti predmetom kaznenog djela ili prekršaja, koji mogu poslužiti za izvršenje kaznenog djela ili prekršaja, premeta koji se mogu koristiti za oštećenje ili uništenje štićenog objekta i predmeta podobnih za napad ili samoozljeđivanje, zaštitar oduzima i privremeno zadržava do predaje policiji ili po završetku postupka vlasniku
- mjesto izvanrednog događaja osigurava do dolaska policije tako da zaštiti i sačuva tragove izvršenja i ne dozvoli nastupanje promjena zatečenog stanja. O stanju i činjenicama, poduzetim radnjama, promjenama na mjestu događanja, oduzetim predmetima i zadržanim osobama usmeno izvješćuje policiju

- tijekom obilaska, kad zaštitar primjeti osobu koja priprema izvršenje krivičnog djela, u tijeku je izvršenja ili je pri odlasku te svojim ponašanjem, djelovanjem ili propustom dovodi u opasnost svoju sigurnost, sigurnost zaštitara ili drugih osoba i imovine unutar štićenog objekta, dužan je primjeniti ovlasti koje su mu dopuštene
- zaštitar će primjeniti tjelesnu snagu ako prethodne mjere i zapovijedi ne jamče uspjeh, uz najblaže posljedice za prekršitelja. Uporaba tjelesne snage prestaje kada napad ili otpor prekršitelja prestane. Kod moguće ozljede prekršitelja, zaštitar će bez odgode pružiti prvu pomoć i po potrebi organizirati liječničku pomoć
- o svim izvanrednim događanjima, zaštitar trenutačno reagira sukladno svojim ovlastima i ovom naputku, izvještava odgovorne osobe i sačinjava izvješće o ID za zaštitarsku tvrtku ili prijavu o uočenom propustu za tvrtku korisnika.
- obavlja ostale poslove zaštitarske službe sukladno znanju i potrebama te zahtjevima korisnika
- vodi odgovarajuće evidencije i knjigu evidencije o primopredaji poslova tjelesne zaštite prema zahtjevima zaštitarske tvrtke i tvrtke korisnika
- na prijemu smjene kao i tijekom obnašanja dužnosti zaštitaru je strogo zabranjeno konzumiranje alkohola i opojnih droga
- u tijeku smjene zaštitaru nije dozvoljeno napuštanje naloženog radnog mjesta unutar štićenog objekta dok mu ne dođe zamjena
- u toku smjene zaštitaru je zabranjeno gledanje TV-a ili korištenje drugih sredstava koja odvlače pozornost sa štićenog objekta
- nije poželjno sklapanje prisnih poznanstava s djelatnicima štićenog objekta i posjetiteljima izuzev kontakata koja se tiču radnih obaveza, niti primanje privatnih posjeta u toku radnog vremena
- zadržavanje stranih osoba u objektima porti nije dozvoljeno duže od trajanja riješavanja provjere identiteta i sačinjavanja propisane ulazne dokumentacije. Također, u porti nije dozvoljeno primanje, čuvanje ili skladištenje drugih materijala i opreme u vlasništvu tvrtke i djelatnika tvrtke
- tijekom provedbi svih radnji sa i prema drugim osobama – djelatnicima pivovare, strankama, posjetiteljima, izvođačima radova vršiti prosudbu izgleda i

ponašanja, vidna alkoholiziranost, vidno psiho – fizičko rastrojstvo te reagirati sukladno tome.

2) posebne dužnosti zaštitara

- tijekom čitavog radnog vremena i u svim situacijama, u okviru perimetra voditi računa o provođenju mjera opće sigurnosti, zaštite na radu, vatrogasne zaštite, zaštite zdravlja i zaštite okoliša, trenutno otklanjati nedostatke, a u slučaju nemogućnosti tražiti pomoć od odgovorne osobe
- nadzirati strogu zabranu pušenja u cijelom krugu tvornice osim na mjestima za pušenje
- nadzirati strogo poštivanje uporabe zaštitnih sredstava: reflektirajući prsluk, kaciga, cipele za zaštitnom metalnom kapicom na mjestima gdje su obavezni, upozoravati na propuste, a kod uočenih opetovanih kršenja naloženih propisa odlučno reagirati
- nadzirati zabranu fotografiranja unutar kruga tvornice bez dopuštenja odgovornih osoba
- nadzirati zaštitu utovarene robe na teretnim vozilima kod kretanja između dva utovarna mjesta, podizanje stranica, navlačenje cerade i postavljanje zaštitnih bočnih pregrada
- posebnu pozornost posvetiti vidljivim neispravnostima na motornim vozilima: curenje tekućina, neispravnosti prtljažnog prostora, iskrenje na električnim instalacijama, ne dozvoliti nikakve radove na održavanju vozila osim trenutnog osposobljavanja za izlazak van kruga, uz obavezno izvještavanje voditelja pogona gdje se neipravnost dogodila
- nadzire vozila koja utovar - istovar vrše povezivanjem na fiksnu ili fleksibilnu instalaciju da su priključena kliješta s izoliranim vodičem te uključena pripadajuća sklopka.
- najefikasnije spriječavati ostavljanje ili ispuštanje bilo kakvog krutog ili tekućeg otpada i matrijala unutar kruga ili u interni sustav odvodne tvornice
- vršiti regulaciju prometa prema prometnim propisima tvrtke te omogućiti sigurno i nesmetano odvijanje prometa uz nužno poštivanje horizontalne i

vertikalne signalizacije, brzine kretanja, uporabu mobitela u tijeku vožnje, pravilnost parkiranja i svih ostalih općih i internih prometnih propisa

3.2.8. Aktivnosti vezane za implementaciju sustava

Sukladno pravilniku o uvjetima i načinu provedbe tehničke zaštite podrazumijeva:

- snimku postojećeg stanja štićenog objekta i analizu problema s ocjenom
- izradu prosudbe ugroženosti
- izradu sigurnosnog elaborata
- definiranje projektnog zadatka
- projektiranje sustava tehničke zaštite
- izvedbu sustava tehničke zaštite
- stručni nadzor nad izvedbom radova
- obavljanje tehničkog prijama sustava tehničke zaštite
- održavanje i servisiranje sustava tehničke zaštite
- uporaba sustava tehničke zaštite.

3.2.8.1. Izrada prosudbe ugroženosti,sigurnosnog elaborata i projektiranje sustava tehničke zaštite

Projektiranje tehničke zaštite povjereno je za to ovlaštenim tvrtkama sukladno Zakonu i o navedenoj djelatnosti potpisan je ugovor sa dvije tvrtke. Ono se mora obavljati u skladu sa važećim zakonima, pravilima struke i poštujući koncept zaštite institucije. Prije same implementacije potrebno je da projektant prezentira tehničko rješenje za pojedini objekt kako bi investitor mogao na vrijeme zatražiti dorade prema specifičnostima objekta.

U sklopu projektiranja izvode se slijedeće radnje:

1. Prosudba ugroženosti i elaborat mjera sigurnosti
2. Izvedbeni projekt sustava tehničke zaštite
3. Projekt izvedenog stanja

Bitan dio projektiranja sustava tehničke zaštite je prosudba ugroženosti, jer se sve kasnije nadovezuje na istu, a iz nje proizlazi i kategorizacija objekta koja nameće određene mjere zaštite. Izrada prosudbe ugroženosti izvodi se na bazi općih i posebnih podataka o predmetnom objektu. Ti podaci se odnose na: vrstu, namjenu i izgled, veličinu, broj prostorija, smještaj objekta (lokacija) i položaj u odnosu na okruženje, pristupne putove objektu, opća građevinska obilježja, postojeću infrastrukturu, blizinu policije, vatrogasaca ili zaštitarskih tvrtki, vrstu aktivnosti koje se u objektu obavljaju, visinu vrijednosti robe koja se u objektu nalazi, broj ljudi koji se povremeno ili stalno nalaze u objektu. Prosudba ugroženosti izrađuje se primjenom priznatih pravila u provedbi tehničke zaštite. Priznata pravila u provedbi tehničke zaštite, u smislu ovoga Pravilnika, su odgovarajuće hrvatske norme, a u nedostatku hrvatskih normi primjenjuju se odgovarajuće europske, odnosno međunarodne norme (EN, IEC, ISO), odnosno druge specijalizirane norme te prihvaćena pravila struke. Iznimno u slučaju manjih nadogradnji moguće je izraditi samo izvedbenu skicu dogradnje sustava, ali se kasnije promjene moraju evidentirati u projektu izvedenog stanja. Faze izrade prosudba ugroženosti i elaborata mjera sigurnosti:

1. Priprema projekta

Priprema projekta podrazumijeva dogovore s predstavnicima tvrtke o krajnjem cilju elaborata i njegovom sadržaju. Nakon prihvaćanja ponude projekta s definiranim obimom i sadržajem pristupa se izradi pripremne dokumentacije koja obuhvaća obrasce za prikupljanje podataka vezanih za sigurnost i kvalitetu. To su kontrolne liste s nizom pitanja koja se odnose na predmetnu problematiku. Obzirom da su tvrtke različite postoji potreba za stalnom revizijom standardnih obrazaca u smislu dobivanja pitanja vezanih za djelatnost tvrtke. Uz to u pripremnoj fazi dogovara se osnovni oblik i terminski plan provedbe prikupljanja podataka.

2. Prikupljanje podataka

Prema normi HRN EN ISO 10011 koja se odnosi na reviziju podaci se prikupljaju u tri koraka; revizija dokumentacije, revizija odgovorne osobe i revizija na licu mjesta.

3. Obrada prikupljenih podataka

Nakon obavljenih istraživanja pristupa se obradi podataka. Cilj obrade je dobivanje sažetog prikaza stanja s mjerama potrebnim za povećanje mjera sigurnosti. Iz ispunjenih obrazaca postaju vidljivi uzroci ugroženosti, a po evidentiranju mogućih izvora ugrožavanja napravljena je analitika rizika i procjena vjerojatnosti pojave štete.

4. Pisanje izvješća

Kada su svi podaci prikupljeni slijedi pisanje izvješća koji sadrži prikaz građevinskih karakteristika objekta, organizaciju sigurnosti, stanje dokumentiranosti, identifikaciju opasnosti, analizu opasnosti i mjere poboljšanja.

5. Prijedog mjera

Prijedlog mjera radi se tako da se na osnovu stvarnog stanja i razlike od očekivanog tj. željenog stanja zaštite na objektu predlože pojedini projektni zadaci za sustave tehničke zaštite koji predviđaju poboljšanje zaštite uz mogućnosti povezivanja s postojećim sustavom.

Izvedbeni projekt mora sadržavati točne dispozicije elemenata sustava tehničke zaštite, raspored opreme u tehničkoj sobi objekta kao i sve bravarske i stolarske elemente na koje se ugrađuju elementi zaštite. Osim navedenog još se za svaki objekt posebno izrađuje skica izvedenog stanja u kojem mora biti ucrtane mikrolokacije svih samouslužnih uređaja sa oznakama vrste i elementima tehničke zaštite koji se na njih montiraju.

3.2.8.2. Izvođenje

Izvođenje sustava tehničke zaštite podrazumijeva izvedbu instalacija, ugradnju uređaja i opreme, programiranje, podešavanje i ispitivanje sustava, verifikaciju uređaja, opreme i sustava koja se obavlja puštanjem u probni rad i izdavanjem certifikata, te izradu uputa za uporabu i obuku osoblja. Izvođenju sustava prethode pripremni radovi koje mogu obavljati i osobe koje nisu registrirane za ugradnju sustava tehničke zaštite sve do spojnih točaka s tehničkim elementima. Kako su svi projekti klasificirani oznakom „tajno“ ili „vrlo tajno“ za potrebe radova na instalacijama se izrađuju posebni nacrti na kojima su ucrtane trase i tipovi kablova koje je potrebno izvući na mikrolokacije bez oznaka elemenata sustava. Instalacije tehničke zaštite moraju biti izvedene sukladnopropisima koji uređuju uvjete izvedbe elektrotehničkih instalacija. Nakon izvedbe i ispitivanja postavljenih instalacija tehničke zaštite ugrađuju se uređaji i oprema. Uređaji i oprema ugrađuju se i podešavaju sukladno projektnoj dokumentaciji i uputama proizvođača uređaja i opreme. Ispitivanje uređaja i opreme, odnosno sustava tehničke zaštite koji su ugrađeni u objekt obavlja se puštanjem u probni rad, a ispravnost se potvrđuje potom izdanim certifikatom. Obuku osoblja koje će upravljati sredstvima, napravama ili sustavima tehničke zaštite provodi pravna osoba ili obrtnik koji ugrađuje sustav. On je također zadužen za isporuku pisanih uputa za pojedini sustav. Osim same verifikacije ispravnosti uređaja na objektu obavezno se ispituje dojava odnosno komunikacija sa dojavnim centrom koji mora zaprimiti dojavu sa svake pojedine zone detekcije na objektu. O ovom ispitivanju dojavni centar izdaje zapisnik koji je dio primopredajne dokumentacije.

3.2.8.3. Nadzor nad izvođenjem

Sukladno Zakonu o privatnoj zaštiti poslove nadzora nad izvođenjem radova tehničkih zaštitnih sustava, revizije projektne dokumentacije tehničkih zaštitnih sustava, tehničkog primitka te pružanja intelektualnih usluga u području tehničke zaštite može obavljati zaštitar – tehničar koji ima završenu visoku stručnu spremu. Predmetna proizvodna tvrtka ugovorila je posao stručnog nadzora sa dvije tvrtke koje imaju ovlast za ovakve poslove. Njihova zadaća je

da prate svaku implementaciju sustava već od samog pregleda izvedbenih projekata i uvođenja instalatera u posao pa do primopredaje sustava i verifikacije okončanog financijskog razračuna. Nadzor nad izvođenjem uključuje:

- nadzor nad implementacijom u smislu poštivanja pravila struke i Zakona
- praćenje terminskog plana izvođenja i usklađivanju radova sa ostalim izvođačima na gradilištu
- izvještavanje investitora o stanju na svim objektima koje nadzire u obliku tjednih izvješća
- nadzor nad poštivanjem koncepta zaštite po kojem se sustavi moraju izvoditi
- nadzor nad provođenjem mjera zaštite od požara i zaštite na radu prilikom implementacije sustava
- sudjelovanje u primopredaji sustava te prikupljanje sve potrebne dokumentacije i atesta za opremu
- tehnički pregled izvedenih radova te kontrole otklanjanja nedostataka u zadanom vremenu
- upisivanje tijeka radova i komentara nadzora u građevinski dnevnik
- sudjelovanje u koordinaciji prilikom izmjena u projektu
- pregled utrošenog materijala i opreme kao i financijska verifikacija okončanih situacija

3.2.8.4. Primopredaja sustava

Po obavljenoj implementaciji, a prije početka korištenja sustava mora se sukladno Zakonu izvršiti primopredaja sustava. Ovo izvode predstavnici izvođača, investitora i ugovorenog nadzora nad izvođenjem. U sklopu primopredaje izdaju se potvrde o obuci korisnika, popis kartica kontrole pristupa sa pristupnim nivoima, popis sigurnosnih ključeva, te se predaju svi certifikati za opremu. Nakon izvršene primopredaje izvođač izdaje vlasniku ili korisniku objekta potvrdu da je sustav tehničke zaštite izveden sukladno odredbama Pravilnika o uvjetima i načinu provedbe tehničke zaštite. Sastavni dio potvrde (prilog 1.) je i zapisnik (prilog 2.) o obavljenom tehničkom prijemu, a propisani

obrazac za oba dokumenta dan je u pravilniku. Na potvrdu se upisuje kategorija objekta sukladno Pravilniku koju je odredio projektant sustava u sklopu prosudbe ugroženosti. U zapisnik nadzor upisuje eventualne nedostatke na sustavima i rok za njihovo otklanjanje, a potvrdu njihovog otklanjanja mora također nadzor verificirati ponovnim pregledom.

3.2.8.5. Održavanje i uporaba

Sukladno Zakonu o privatnoj zaštiti sustavi tehničke zaštite moraju se održavati jednom godišnje. Poslove održavanja investitor je dužan ugovoriti sa tvrtkom licenciranom za poslove tehničke zaštite, a tvrtka je dužna sukladno ugovoru izdati zapisnik o redovnom pregledu i upisati stanja svih sustava u knjigu održavanja. Analizirana tvrtka vrlo strogo poštuje ugovor i zakone te prema tome izvršava redovna održavanja. U sklopu ugovora o održavanju dan je popis svih lokacija objekata i propisani su radovi koji se izvode prilikom redovnog održavanja. Osim navedenog održavanja izvođač je dužan osigurati održavanje i servisiranje sustava u jamstvenom roku, a na zahtjev korisnika ponuditi održavanje i servisiranje izvan jamstvenog roka, te omogućiti isporuku potrebnih pričuvnih dijelova u razdoblju pet godina od dana puštanja sustava u rad.

4. REZULTATI I RASPRAVA

Analizom je utvrđeno da sustavi implementirani na objektima promatranog investitora vrlo dobro prate promjene zakonske regulative i razvoj novih tehnologija te da su implementirani sustavi visoke kvalitete sa malo potreba za servisom odnosno popravcima. Kako je razvoj novih tehnologija sve brži potrebno je što češće sagledati koncept zaštite i implementirane sustave i prosuditi postoji li opravdani razlog o uvođenju novih tehnologija. Primjerima je prikazano kako se može unaprijediti pojedini sustav kako slijedi:

1) Protuprovalni sustav

- pošto se u krugu tvrtke nalaze veliki objekti, posebno skladišta sa gotovom robom, a na nijednom nema protuprovalni detektor, rizik od krađe je povećan. No tu se ne radi o krađi poput pokušaja iznošenja već o konzumiranju gotovih proizvoda. Mnogo je vanjskih izvođača unutar kruga tvrtke i povećan je rizik od znatiželjnih i "žednih" radnika. U jutarnjoj i popodnevnoj smjeni veliki je protok radnika pa je za to vrijeme najbolje postaviti video nadzor sa detektorima za lom stakla sa što nižom frekvencijom loma kako bi se moglo detektirati korištenje staklene ambalaže (udaranje boca o bocu)
- proceduralno je potrebno propisati da se sve šifre na protuprovalnim sustavima mijenjaju jednom godišnje prilikom redovnog pregleda sustava
- kod ranije spomenutog šatora potrebno je postaviti PIR detektor na baterije sa kamerom

2) Videonadzor

Na sustavima video nadzora kao i na protuprovalnim sustavima zadovoljeni su svi zakonski minimumi kojih se proizvodna tvrtka mora pridržavati no i ovdje se može bitno poboljšati razina sigurnosti ovisno o financijskim mogućnostima investitora. Predložene su slijedeće mjere za poboljšanje:

- pokretne kamere ugrađene ispred pojedinog objekta nisu isto parametrirane pa bi trebalo odrediti način programiranja preseta po kojima se kamera kreće kao i promjene istih u slučaju alarma

- konceptom nije detaljno dobro opisano parametriranje sustava video nadzora (kvaliteta zapisa, broj slika u sekundi) pa sustavi nisu jednako parametrirani. Potrebno je detaljnije opisati zahtjeve investitora za pojedine vrste kamera i pozicije koje štite kako bi svi sustavi bili standardizirano programirani, a ne prepušteni na volju instalatera
- potrebno instalirati megapikselne kamere koje osiguravaju kasniju bolju digitalnu obradu i analitiku snimljenog materijala. Za to se podrazumijeva zona u kojoj je šator sa robom za izvoz te kod obje porte kako bi bila snimljena registracijska tablica svih vozila koje ulaze
- potrebno je razmotriti ugradnju dodatnih reflektora koji bi osvjetljavali perimetar tvrtke. Također i unutarnja rasvjeta na nekim mjestima nije zadovoljavajuća pogotovo u noćnoj smjeni, tako da za unutarnje kamere treba postojati minimalna nužna rasvjeta. Ovo je moguće riješiti ugradnjom IC reflektora, odnosno doradom razvodnih ormara rasvjete koja bi uvijek bila uključena.

Sigurnost video nadzora

U umreženosti leži sigurnosni problem, jer proizvođači opreme prodaju sustave video nadzora s omogućenim pristupom na Internet i na žalost prilično niskom razinom zaštite. Unatoč činjenici da sustavi videonadzora posjeduju mogućnost lozinke iste su tipizirane i solidno dokumentirane što znači da svi oni koji žele pristupiti sustavima video nadzora koji su priključeni na internet to mogu učiniti vrlo jednostavno, isprobavajući nekoliko tipiziranih lozinka. Kroz analizu sustava pokazalo se da su sustavi video nadzora loše zaštićeni zbog tvorničkih postavki sustava koji uključuju omogućen pristup s Interneta i jako slabe lozinke. Osim toga to znači isto da se za pristup takvim sustavima videonadzora ne moraju baviti hakeri, jer pristupiti sustavima videonadzora može praktički bilo tko. Osim toga ranjivosti sustava pridonose i informacije objavljene na internetu na kojem je objavljena web stranica koja posjeduje poveznice brojnih nadzornih kamera koje nisu zaštićene. Moderniji i kvalitetniji sustavi jednako su podložni hakerskim napadima upravo zbog činjenice da se ne mijenjaju tvorničke lozinke i postavke. To omogućuje kontrolu nad video nadzorom. Međutim, spriječiti

takve napade nije toliko složeno koliko se na prvi pogled čini. Prvi korak je poduzimanje mjera da se osobama za održavanje i upravljanje sustavima videonadzora prepusti da se sustav konfigurira prema pravilima struke. To znači da se najprije uklone tvorničke postavke, promijene podrazumijevane lozinke i pri tome promijene korisnička imena u nešto što će potencijalni napadači teže pogoditi. Za stjecanje kontrole na bilo kojim sustavima pa tako i na sustavima videonadzora koriste se maliciozne računalne skripte koje u vrlo kratkom periodu iskušavaju razne kombinacije lozinki i korisničkih imena pri čemu se prve isprobavaju tvorničke lozinke i korisnička imena. Jasno je da će sustav koji nema promijenjene tvorničke postavke biti vrlo brzo i bezbolno kompromitiran te kao takav može biti ulazna točka za pristup drugim dijelovima sustava. Drugi korak je onemogućavanje pristupa sustavu s Interneta ili rekonfiguracija sustava. Obzirom da je udaljeni pristup vrlo koristan potrebno je rekonfigurirati sustav tako mu se može pristupiti isključivo iz lokalne mreže ili vpn-om. Takvom rekonfiguracijom sustav neće biti javno dostupan nego će biti dostupan samo ovlaštenim osobama.

3) Sustav kontrole prolaza i mehaničke zaštite

Kako sustavi kontrole prolaza zakonom nisu definirani do u detalje na predmetnim objektima svi sustavi su zadovoljavajući jer ispunjavaju uvjete za najzahtjevnije prostore. Sustav kontrole prolaza sa beskontaktnim karticama na spomenutim objektima funkcionira besprijekorno, a svaki nasilan ulaz bio bi detektiran i alarmiran. Zaštitari odlično obavljaju svoju funkciju na portama te tek kada pregledaju vozilo koje ulazi podižu rampu. Roba u skladištima u stalnom je pokretu te se ne smije ograđivati dodatnom mehaničkom zaštitom (previše bi usporilo proces transporta)

Prijedlog:

Postoje uredi u objektu između proizvodnje kvasca i upravne zgrade te uredi na kraju skladišnog prostora. Ti uredi nemaju ugrađenu kontrolu prolaza beskontaktnim karticama te praktički, ako se ne zaključaju vrata svatko može ući u njih, prema tome se predlaže ugradnja kontrole prolaza za ulaz u te urede.

4) Vatrodojavni sustav

Što se tiče vatrodojavnih sustava oni su apsolutno zadovoljavajući obzirom da su ugrađeni i tamo gdje nisu obavezni kao mjera procjene ugroženosti od požara nego na zahtjev investitora. Jedina mana je ta što postoje dvije vatrodojavne centrale, glavna koja javlja da se dogodilo alarmno stanje i sporedna koja je spojena na nekoliko zona te ona javlja glavnoj centrali alarmno stanje pa se tek onda glavna centrala odaziva.

Prijedlog:

- trebalo bi glavnu vatrodojavnu centralu proširiti tako da se sve zone sa sporedne centrale spoje na glavnu. To će omogućiti sigurniji rad i točnije detektiranje zone u kojoj bi nastalo alarmno stanje. Ako bi bilo potrebno povećat broj javljača požara
- još jedna mana je, ako dođe do požara u skladištima, zaštitari prvo moraju otići na mjesto detekcije da utvrde da li je lažan alarm ili stvarni požar, te ukoliko ne mogu samostalno ugasiti vatru sa aparatom za gašenje, tek onda javljaju JVP potvrdu dolaska, a za takvu situaciju se predlaže postavljanje okretnih kamera kako bi zaštitari odmah sa nadzornog mjesta mogi ustanoviti razinu opasnosti te ne bi gubili vrijeme do dolaska na mjesto nastanka alarma

5) Tjelesna zaštita

Na promatranim lokacijama gdje djeluje tjelesna zaštita uočeno je da se prema pravilima struke izvršavaju sve procedure vezane na tjelesnu zaštitu. Kao opasku bi trebalo navesti da jedno te isti zaštitari rade na ovoj lokaciji i to minimalno dvoje u paru po smjeni te su uvijek u istim parovima. Dužim radom zaštitara na istoj lokaciji može doći do prijateljskih odnosa sa zaposlenicima što nije preporučljivo za njihovo radno mjesto. Također, ako zaštitari stalno rade u istim parovima, postaju bliski te ukoliko dođe do njihovog propusta štitit će jedno drugo.

Prema tome se navode sljedeći prijedlozi:

- ukoliko zaštitarska tvrtka pruža usluge na drugim lokacijama u gradu, bilo bi poželjno razmjenjivati svoje zaštitare na tjednoj bazi
- bilo bi poželjno mijenjati parove po smjenama

6) Općenite mjere poboljšanja zaštite
- ugovorom je potrebno definirati redovito ažuriranje procedura kretanja i prosudbu ugroženosti, definirati u kojim vremenskim razmacima je isto potrebno izvesti.
- kod bilo kakvih promjena pozicije elemenata tehničke zaštite potrebno je te promijene evidentirati u projektu izvedenog stanja kako bi se uvijek znalo pravo stanje na objektu.
- potrebno je uspostaviti sistem distribuiranja uputa zaštitarima, odgovornost za njihovu primjenu i način kontrole njihove primjene.
- na velikim objektima obavezno treba imenovati osobu koja je zadužena za zaposlenike na objektu, njihovo ažuriranje (šifre, kartice, nivoi pristupa) te potpisivanje izvještaja o učinjenim servisima i pokretanje zahtjeva za servisom. Trenutno se ovo radi neorganizirano odnosno svako može pokrenuti zahtjev, a serviser ima odgovornost kome će dati koji pristupni nivo unutar objekta.

Tab. 3 Upit za nadzor i kontrolu zaposlenika i posjetitelja

PITANJE	ODGOVOR DA/NE	NAPOMENA
Da li postoji identifikacijska kartica za svakog zaposlenika?		
Kako se nadziraju i čuvaju prazne identifikacijske kartice?		
Da li postoje ulazi za posjetitelje i vanjske suradnike (opišite)?		
Koliki je dnevni broj posjetitelja na svakom ulazu?		
Da li su posjetitelji i vanjski suradnici za trajanje svog posjeta cijelo vrijeme nadzirani?		

Da li postoji odgovarajuća evidencija sa svim bitnim podacima o posjetiteljima, poslovnim partnerima i vanjskim suradnicima?		
Da li zaposlenici neovlašteno koriste neke od ulaza u štićeni objekt?		
Tko je zadužen za nadzor, kontrolu i evidenciju kretanja zaposlenika i posjetitelja unutar štićenog objekta?		
Da li je dozvoljeno parkiranje osobnih automobila unutar štićenih prostora?		
Da li postoji sustav za evidenciju vozila zaposlenika posjetitelja i vanjskih suradnika (opišite)?		
Da li je do sada bilo incidentnih situacija?		
Kako i u kojem roku su incidentne situacije rješavane?		
Tko je zadužen za intervenciju u takvim situacijama?		

Navedeni upit bio je proslijeđen zaštitarima na obje porte predmetne proizvodne tvrtke. Zaštitari su bez oklijevanja, sa pristojnim i uljudnim ponašanjem prihvatili upit te ga za neko određeno vrijeme ispunili. To je pokazatelj kako ozbiljno shvaćaju svoj posao te ga kvalitetno izvršavaju, jer se već nekoliko godina nije dogodio niti jedan incident.

5. GDPR (General Data Protection Regulation)

U trenutku pisanja ovog Završnog rada, 25. svibnja 2018. na snagu stupa opća uredba o zaštiti osobnih podataka. To je nova europska uredba koja donosi brojne i značajne promjene u pravilima kojima su definirani osobni podaci i način njihova korištenja. Uz to, postavlja i neke osnovne principe koji se odnose na osobne podatke poput toga da oni moraju biti obrađeni u skladu sa zakonom te da se smiju prikupljati samo za određene, izričite i zakonite svrhe. Uredba je obvezujuća i izravno primjenjiva na sve organizacije koje u svom poslovanju koriste osobne podatke, što uključuje organizacije unutar Europske unije, ali i sve organizacije izvan Europske unije koje se koriste osobnim podacima unutar EU. Iako je stupila na snagu još 24. svibnja 2016., u punoj primjeni je od 25. svibnja 2018. Prijelazni period od dvije godine služio je da bi organizacije imale dovoljno vremena izraditi plan implementacije i usklađivanja s Uredbom, alocirati potrebne resurse te odraditi taj projekt. Da bi se uskladili s GDPR-om, većina hrvatskih tvrtki trebala je prilagoditi svoje postojeće procedure i ustanoviti nove, ali i iz temelja promijeniti poslovne sustave koje koriste. Edukacija zaposlenika je u početku bila izborna, no međutim zbog prirode nove Uredbe, ona je ubrzo postala neizbježna. Osobni podaci morat će se obrađivati sukladno zakonu i prikupljati samo za određene, eksplicitne svrhe, a prikupljeni podaci moraju biti minimizirani, točni i ažurni. Obrada podataka vršit će se na način koji osigurava odgovarajuću sigurnost i zaštitu od neovlaštenog ili nezakonitog postupanja i slučajnog gubitka, uništavanja ili oštećenja, koristeći odgovarajuće tehničke ili organizacijske mjere. U slučaju povrede ili zloupotrebe podataka, tvrtka će morati obavijestiti Regulatornu agenciju (AZOP) pa čak i pojedince na koje se to odnosi, u roku od 72 sata od identifikacije kršenja. Takav scenarij može rezultirati novčanim kaznama od 20 milijuna eura ili do 4% godišnjeg prometa, koje bi tvrtka morala pretrpjeti. Novo načelo odgovornosti zahtjeva da se dokaže usklađenost sa svim dijelovima uredbe i eksplicitno kaže da je to obaveza tvrtke. Očekuje se da tvrtka osigura sveobuhvatne ali odgovarajuće mjere

upravljanja. Mjere koje minimiziraju rizik zloupotrebe i štite osobne podatake. Data Protection Officer ili Službenik za zaštitu osobnih podataka nova je uloga koja je uvedena u organizacijsko okruženje tvrtki. Neke od njegovih odgovornosti je upravljanje politikama tvrtke za rukovanje osobnim podacima, podizanje razine svijesti o potrebi zaštite osobnih podataka i osiguranje kvalitete.

5.1. Što GDPR donosi pojedincu?

Pojedincu se vraća potpuna kontrola upravljanja vlastitim osobnim podacima koje poslovni subjekti sakupljaju o njemu. Sve u svrhu stvaranja većeg povjerenja između pojedinaca i tvrtki uz visoku razinu transparentnosti u korištenju osobnih podataka. Pojedinac ima pravo na uvid u osobne podatke i način na koji se koriste – što se zove pravo pristupa subjektu. Pojedincu je također omogućeno zatražiti da se njegov paket osobnih podataka "prenese" drugom dobavljaču robe ili usluge – što se naziva pravo prenosivosti podataka. Sve obrade osobnih podataka moraju biti osigurane pravnom osnovom. Privola predstavlja jednu od pravnih osnova, a GDPR propisuje da definicija privole treba biti jasna, nedvosmislena i specifična te se privola mora moći jednostavno i opozvati. Pojedinci će imati pravo tražiti da kompanije obrišu sve njihove osobne podatke za koje ne postoji uvjerljiv razlog za nastavak procesiranja. Ovo pravo nije apsolutno, jer postoje zakonska ograničenja za brisanje podataka, te je bitno razlikovati legitimne osnove za procesiranje. Primjer kada se ovo pravo primjenjuje je kada pojedinac ukine privolu ili kada njegovi osobni podaci više nisu nužni za ispunu svrhe.

6. ZAKLJUČAK

Zadatak Završnog rada obuhvaćao je opis i analizu koncepta zaštite proizvodne tvrtke te je zahtjevao obilazak svih njenih objekata, ispitivanje i potražnja informacija kod osoba zaposlenika te tvrtke i tvrtke pružatelja usluge tjelesne i tehničke zaštite. Dostupnost podataka uvelike je olakšala i stručna praksa koja je bila obavljena u predmetnoj tvrtci. Opis i analiza koncepta zaštite proizvodne tvrtke zahtijeva određena stručna znanja o implementaciji sustava tehničke zaštite i znanja legislative koja pokriva predmetno područje koje se akumulira kroz niz stručnih seminara s temama tehničke zaštite i legislative područja tehničke zaštite.

Analizom svih aspekata sigurnosti na objektima proizvodne tvrtke utvrđeno je da su implementirani sustavi tehničke zaštite iznad prosjeka kvalitete i složenosti u odnosu na većinu proizvodnih tvrtki u Hrvatskoj. Posebno treba napomenuti kako je pružanje tjelesne zaštite i rad zaštitara na visokom nivou što je i očekivano, jer su oni najodgovorniji za sprječavanje nedozvoljenih aktivnosti unutar perimetra tvrtke. Predmetna proizvodna tvrtka je po financijskim rezultatima među najuspješnijima u državi, gledano sa financijske strane, puno lakše ispunjava zadane uvjete nego ostale tvrtke u Hrvatskoj. Naveden je niz prijedloga, mjera i preporuka, jer uvijek postoji bolja zaštita od implementirane, a pitanje je samo ostvaruje li se njome i bolji učinak odnosno opravdava li cilj sredstvo ili bi navedena poboljšanja bila samo dodatni trošak bez velikog učinka na stanje sigurnosti. Brzi razvoj novih tehnologija i pad cijena na tržištu osigurava buduću primjenu raznih izvedbi uređaja i detektora za povećanje opće sigurnosti pa se shodno tome Koncepti zaštite redovno moraju revidirati i pomalo uvoditi nove tehnologije i sustave i to u trenutku kad oni mogu dati najbolje rezultate.

Tvrtka je educirala svoje zaposlenike i pripremila ih za GDPR, te teoriju što više pokušava pretvoriti i u praksu. Bez obzira na kompleksnost implementiranog sustave tehničke zaštite i bez obzira na uložena sredstva isti sustavi samostalno ne mogu dati zadovoljavajuće rezultate bez ljudskog faktora. Odgovorna osoba brine se o svim komponentama sustava, kontrolira ih,

servisira, testira, sustavno razmišlja o unapriјeđenjima zaštite, stvara pravilnike, procedure, strategije, politike i ostale dokumente za cijelovito upravljanje sigurnosti u ovakvoj proizvodnoj tvrtci.

7. LITERATURA

[1] Dešlimunović D.: *''Suvremeni koncepti i uređaji zaštite''*, I.T. Graf, Zagreb, (2002.)

[2] Dešlimunović D.: *"Menadžment zaštite i sigurnosti"*, Pragmatekh, Zagreb, (2006.)

[3] Nađ I., Paić K., Ribičić G., Maršić M., Pintar B., Vasilj P.: *"Priručnik za izobrazbu čuvara i zaštitara"*, Veleučilište Velika Gorica, Velika Gorica, (2013.), 978-953-7716-40-0

[4] Bilješke iz kolegija *''Alarmni sustavi''*, dr.sc. Vladimir Tudić, prof. visoke škole, Veleučilište u Karlovcu, Karlovac, (2017/18.)

[5] http://www.sbo.hr/proizvodi/tehnicka-zastita-prostora-neprobojnost/26/?gclid=EAIaIQobChMImJuH2fab2gIVTzwbCh0bxAszEAAYASAAEgKMG_D_BwE, pristupljeno 3.4.2018.

[6] http://sigurnosni-sustavi.hr/alarmni-sustavi/, pristupljeno 6.4.2018.

[7] https://living.vecernji.hr/interijeri/alarmi-su-sve-sofisticiraniji-i-nije-ih-lako-probiti-kao-u-akcijskom-filmu-964286, pristupljeno 10.4.2018.

[8]http://www.riteh.uniri.hr/zav_katd_sluz/zae/as/download/Alarmni%20sustavi%2014&15.pdf, pristupljeno 15.4.2018.

[9] https://www.alarmautomatika.com/documents/files/promo/09060-Vodic-kroz-provjerena-rjesenja-tehnicke-zastite.pdf, pristupljeno 16.4.2018.

[10]https://www.mup.hr/UserDocsImages/SAVJETOVANJE/2013/zozni/PRAVILNIK_O_TEH_ZASTITI_.pdf, pristupljeno 5.4.2018.

[11] http://www.maturskiradovi.net/forum/Thread-sistemi-protuprovalne-za%C5%A1tite-hr, pristupljeno 21.4.2018.

[12] https://www.alarmautomatika.com/hr/elektronicka-zastita-artikala/21/, pristupljeno 2.5.2018.

[13] https://www.scribd.com/doc/95286635/Alarmni-Sustavi-Seminar, pristupljeno 10.5.2018.

[14] http://pragmatekh.hr/pdf/Trailer.pdf, pristupljeno 11.5.2018.

[15] file:///C:/Users/Ivan/Downloads/608_tehnomobil-ae-inovativan-pristup-sigurnosti.pdf, pristupljeno 14.5.2018.

[16] http://www.propisi.hr/print.php?id=14434, pristupljeno 20.5.2018.

[17] https://lider.media/znanja/krada-u-tvrtki-osim-sto-pretrpe-stetu-poduzetnici-moraju-platiti-pdv-na-manjak/, pristupljeno 21.4.2018.
[18] http://stubovi.co.rs/statistike-kradje-u-malim-i-srednjim-preduzecima/, pristupljeno 5.5.2018.
[19] http://www.dom.com.hr/gradjevinski-radovi/instalacije/sigurnosne-instalacije/alarmi/pojmovnik-alarmnih-sustava.dom, pristupljeno 1.6. 2018.
[20] https://www.google.hr, pristupljeno 10.7.2018.
[21] https://www.algebra.hr/cjelozivotno-obrazovanje/gdpr-kako-uskladiti-poslovanje-s-novom-uredbom-europske-unije/?gclid=EAIaIQobChMIvNKs2 https://dataprivacymanager.net/hr/gdpr/?gclid=EAIaIQobChMIkNenhOHE3AIVRLTtCh2IBQJyEAAYASABEgJkxPD_BwE, pristupljeno 23.7.2018.
[22]http://www.hzn.hr/UserDocsImages/glasila/Oglasnik%20za%20normativne%20dok_5_2016-kor1.pdf, pristupljeno 14.4.2018.
[23] Plan osiguranja pivovare Heineken Hrvatska d.o.o.
[24] Postupak zaštitara kod aktivacije vatrodojavnog alarma pivovare Heineken Hrvatska d.o.o.

8. PRILOZI

8.1. Popis slika

8.2. Popis tablica

8.3. Popis priloga

Prilog 1. Potvrda o izvedbi sukladno sa Pravilnikom o uvjetima i načinu provedbe tehničke zaštite

_____

(NAZIV I SJEDIŠTE TRGOVAČKOG DRUŠTVA ILI OBRTNIKA)

Na temelju članka 22. stavka 4. Pravilnika o uvjetima i načinu provedbe tehničke zaštite ("Narodne novine", br. __/__.) izdaje se

P O T V R D A

kojom se potvrđuje da je izvedba sustava tehničke zaštite, prema Ugovoru broj: _____,
(broj Ugovora)
sklopljenog s naručiteljem posla _____, koji je u svojstvu
(naziv pravne ili fizičke osobe)

vlasnika/korisnika/_____ (drugo) objekta iz _____
(podcrtaj ili upiši) (sjedište pravne osobe ili adresa fizičke osobe)

obavljena sukladno odredbama uvodno navedenog Pravilnika.

Štićeni objekt je sukladno članku 6. stavku 4. navedenog Pravilnika svrstan u _____ kategoriju.

Sastavni dio ove potvrde je zapisnik o obavljenom tehničkom pregledu sustava tehničke zaštite.

Ova se potvrda izdaje u dva primjerka - jedan za investitora, a drugi za izvođača koji je pohranjuje u pismohranu trgovačkog društva ili obrta.

_____ M.P. _____
(mjesto i datum) (ovlašteni predstavnik izvođača)

Prilog 2. Zapisnik o tehničkom prijemu

_____

(NAZIV I SJEDIŠTE TRGOVAČKOG DRUŠTVA ILI OBRTNIKA)

Na temelju članka 22. stavka 3. Pravilnika o uvjetima i načinu provedbe

tehničke zaštite ("Narodne novine", br. __/__.) sastavlja se

Z A P I S N I K

o obavljenom tehničkom prijamu naprava i sustava tehničke zaštite prema Ugovoru broj:

_____

(broj Ugovora)

sklopljenog sa:

_____.

(naziv i sjedište pravne osobe ili adresa obrtnika)

Prilikom prijama naprave/uređaja/sustava tehničke zaštite je utvrđeno:

1. da je ugrađena naprava/uređaj/elementi sustava tehničke zaštite u ispravnom stanju i u funkciji za koju su namijenjeni;
2. da je ugradnja naprave ili uređaja izvedena sukladno skici (crtežu);
3. da je sustav tehničke zaštite usklađen sa projektom;
4. da je osoba/osoblje koje upravlja napravom/uređajem/sustavom tehničke zaštite obučeno za taj posao;
5. da su korisničke upute uručene vlasniku ili korisniku objekta i da su iste komplementarne s ugrađenim elementima;
6. da su certifikati i potvrde koje dokazuju kvalitetu ugrađene opreme provjereni i uručeni vlasniku ili korisniku objekta.

U _____

(mjesto i datum)

Za naručitelja: Za izvođača:

_____ _____

(potpis naručitelja) (potpis ovlaštenog predstavnika izvođača)