Tehnička zaštita računalnih sustava

Pavlin, Josip

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

JOSIP PAVLIN

TEHNIČKA ZAŠTITA RAČUNALNIH SUSTAVA

Završni rad

Pula, rujan, 2021. godine

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

JOSIP PAVLIN

TEHNIČKA ZAŠTITA RAČUNALNIH SUSTAVA

Završni rad

JMBAG: 0233005166, izvanredni student

Studijski smjer: Informatika

Predmet: Modeliranje poslovnih procesa

Mentor: doc. dr. sc. Darko Etinger

Pula, rujan, 2021. godine

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani/a Josip Pavlin ovime izjavljujem da je ovaj seminarski rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio seminarskog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student/ica

Ime i prezime

Sadržaj

1. UVOD

U današnje vrijeme se poslovanje odvija u sve većim uvjetima digitalnog okruženja i potreba za smještajem i čuvanjem sve veće količine podataka iziskuje velike i brze sustave koji mogu zadovoljiti sve veće zahtjeve. Uz iznimku velikih firmi i nacionalnih institucija, kojima je isplativije ili nužno imati svoje podatkovne centre, puno je veći broj korisnika kojima nije isplativo imati svoje centre nego iznajmiti prostor ili dio poslužitelja u nekom podatkovnom centru.

Prvenstveno, svrha velikih računalnih sustava je neometan i siguran pristup podacima, gdje se ulaganje u veće sustave pohrane podataka ne isplati jer iziskuje velika izdvajanja. U samom startu potrebno je odvojiti velika sredstva na nabavku opreme, a kasnije i na održavanje i zaštitu te iste opreme. Ako se i korisnik odluči na soluciju nabavke opreme i održavanje iste, iskorištenost takve opreme bude jako malog postotka. Osim zaštite od gubitka podataka, jako veliku važnost ima i zaštita od neovlaštenog pristupa podacima.

Kroz ovaj rad bit će opisana tehnička zaštita računalnog sustava kao sigurnost od neželjenih gubitaka ili dijeljenja podataka. Kako napreduje tehnologija, tako i napreduju sofisticirani načini pomoću kojih se može ostvariti neželjeni događaj, pa se samim tim napretkom i oprema sve više unaprjeđuje.

2. RAČUNALNI SUSTAV

2.1. Povijest

Podatkovni centri vuku korijene iz ogromnih računalnih soba 1940-ih, koje je tipizirao ENIAC, jedan od najranijih primjera podatkovnog centra. Rani računalni sustavi, složeni za rad i održavanje, zahtijevali su posebno okruženje u kojem su mogli funkcionirati. Za povezivanje svih komponenata bilo je potrebno mnogo kabela, a osmišljeni su načini za smještaj i organizaciju, kao što su standardni nosači za montiranje opreme, povišeni podovi i nosači kabela (ugrađeni iznad ili ispod povišenog poda). Glavno računalo zahtijevalo je veliku snagu i morao se hladiti kako bi se izbjeglo pregrijavanje.

Sigurnost je postala važna - računala su bila skupa i često su se koristila u vojne svrhe. Stoga su osmišljene osnovne smjernice za dizajn za kontrolu pristupa računalnoj sobi.

Tijekom procvata mikro računarske industrije, a posebno tijekom 1980-ih, korisnici su počeli postavljati računala posvuda, u mnogim slučajevima s malo ili nimalo brige o operativnim zahtjevima. Međutim, kako su operacije s informacijskom tehnologijom (IT) postajale sve složenije, organizacije su postajale svjesne potrebe za kontrolom IT resursa.

Pojava Unixa iz ranih 1970-ih dovela je do širenja slobodno dostupnih Linux-kompatibilnih operativnih sustava za računala tijekom 1990-ih. Oni su se zvali "poslužitelji", jer se operativni sustavi za dijeljenje vremena, poput Unixa, u velikoj mjeri oslanjaju na model klijent-poslužitelj kako bi olakšali dijeljenje jedinstvenih resursa između više korisnika.

Dostupnost jeftine mrežne opreme, zajedno s novim standardima za mrežno strukturirano kabliranje, omogućila je upotrebu hijerarhijskog dizajna koji je poslužitelje smjestio u određenu prostoriju unutar tvrtke. Upotreba izraza "podatkovni centar", primijenjena na posebno dizajnirane računalne sobe, počela je stjecati popularno priznanje u ovo vrijeme. Nagli porast podatkovnih centara dogodio se tijekom dot-com balona 1997. - 2000.

Tvrtkama je bila potrebna brza internetska povezanost i neprekidni rad kako bi postavili sustave i uspostavili prisutnost na Internetu. Instaliranje takve opreme nije bilo

održivo za mnoge manje tvrtke. Mnoge su tvrtke počele graditi vrlo velike objekte, nazvane internetskim podatkovnim centrima (IDC), koji pružaju poboljšane mogućnosti, kao što je križanje sigurnosnih kopija. [1]

2.2. Dijelovi računalnog sustava

Kroz ovo poglavlje nabrojati će se svaki segment računalnog sustava i opisati kakvih su karakteristika, koji dijelovi služi za što, te njegove prednosti i kvalitete.

Kao primjer koristit će se računalni sustav „DATACROSS JASTREBARSKO“ koji predstavlja jedan od većih domaćih dana centara. „DATACROS JASTREBARSKO“ se nalazi 35 kilometara od Zagreba, u neposrednoj blizini autoceste Zagreb-Karlovac. Kao dio poduzetničke zone, ne postoje elementi koji bi samom svojom lokacijom ugrožavali rad podatkovnog centra ili dovodili u opasnost bilo radnike, bilo objekte tvrtke.

- Tehničke karakteristike lokacije Jastrebarsko:
  - Ukupne kvadrature predviđene za smještaj IT opreme 1.300 m2
  - SLA dostupnost (Tier3) od 99,982%
  - Udaljenost od Zagreba 35 kilometara i smještaj na različitom potresnom području u odnosu na Zagreb
  - Carrier neutral data centar optikom povezan s 2 čvorišta u Zagrebu i vezom na CIX, VIX i BIX
  - Lokacija ima izvrsnu prometnu povezanost sa Zagrebom

- Izvori Napajanja:
  - Dvije različite dalekovodne petlje
  - Redundantna transformatorska postrojenja 4MW
  - Redundantni energetski rasklopni čvorovi

[1] https://en.wikipedia.org/wiki/Data_center

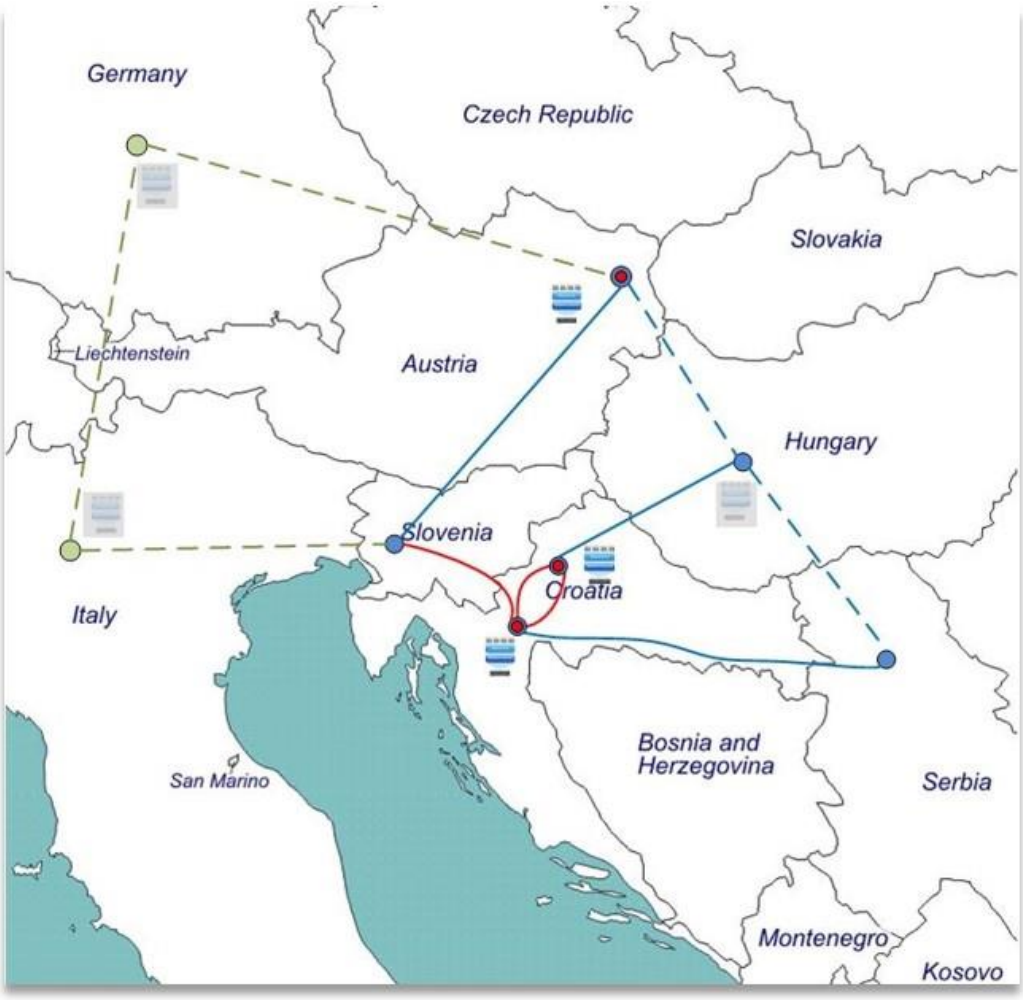
- Dizelski agregati snage 4 x 1,6MW u sinkronom radu (garantiraju neovisnost DC-a 72 sata na punoj snazi)
- Dvije grane napajanje (A+B) obje napajane iz UPS sustava (2N+1)

Slika 1. Izvor napajanja (izvor: https://www.setcor.com/o-nama/podatkovni-centri/#!)

- Rashladni sustav:
  - Redundantne vanjske rashladne jedinice
  - Redundantno strojarsko postrojenje (strojarnice)
  - Hlađenje iz poda (cijeli prostor je pokriven višestrukim redundancijama)
  - U slučaju visoke koncentracije disipacije vrlo jednostavna ugradnja In-row jedinica
  - Velika količina senzora za temperaturu i vlagu u prostoru

- Telekomunikacije:
  - Dvije nezavisne optičke trase do dva odvojena čvora u Zagrebu
  - Kapacitet prijenosa na svakoj trasi 160 x 10 G
  - Fiber Channel (2,4,8,10 G); Ethernet do 10G i sve manje brzine na L2 ili L3

- Odlična međunarodna povezanost na Beč, Budimpešta, Milano, Ljubljana, Beograd,…
- Spoj na CIX čvor za promet unutar Hrvatske



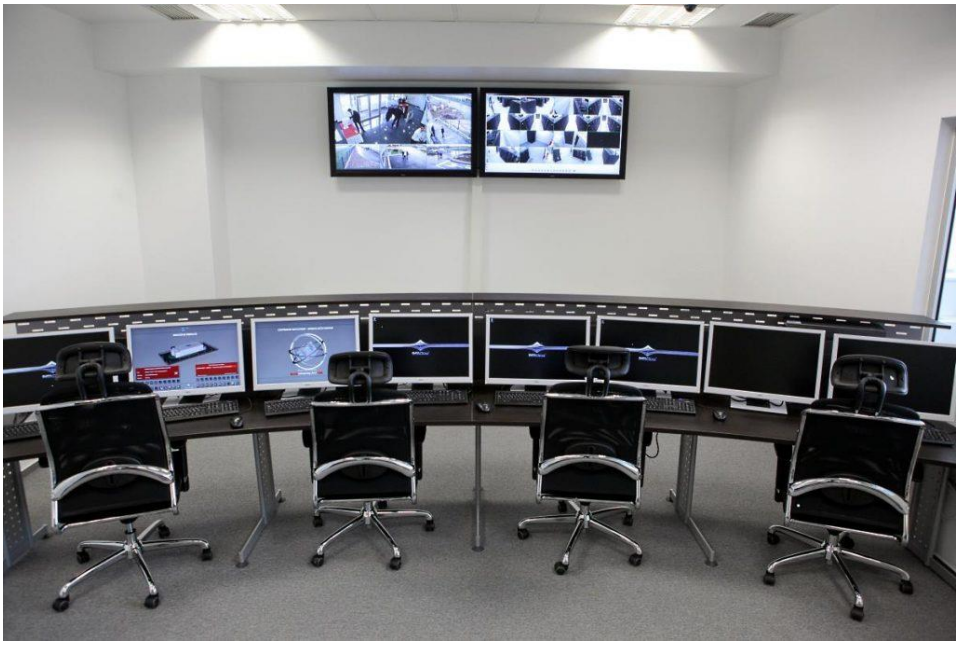
Slika 2. Telekomunikacije (izvor https://mydataknox.hr/o-nama/nasi-data-centri#!)

- Sigurnost i zaštita cijelog kompleksa kao jednog sustava:
  - Protuprovala: sigurnosne zone, perimetarska zaštita, protuprovalni nadzor prostora, video nadzor
  - Kontrola pristupa: biometrijska kontrola i pristup putem kartica

- Vatrodojava: VESDA (Very Early Smoke Detection) I vatrodojavne centrale i detektori požara u nekoliko odvojenih zona
- Vatrozaštita: redundantni sustav gašenja plinom NOVEC uz više požarnih zona
- Fizička zaštita 24/7

Slika 3. Protuprovala (izvor https://mydataknox.hr/o-nama/nasi-data-centri#!)

- Kontrolna soba iz koje se upravlja sustavom kroz udaljenim pristupom serverima.



Slika 4. Kontrolna soba (izvor https://mydataknox.hr/o-nama/nasi-data-centri#!)

- Strukturno kabliranje UTP kablovima Cat 6 (kategorije 6) i SMF i MMD (singlemodni i multimodni) optičkim kablovima.

2.3. Osnovni elementi sigurnosti

Osnovne elemente sigurnosti Računalnih sustava možemo podijeliti grubo podijeliti u dvije grupe:

- Pouzdanost rada računalnih sustava
- Zaštita računalnih sustava

Pod pouzdanošću rada računalnog sustava možemo definirati kao vjerojatnost da sustav radi i ostvaruje u svakom trenutku sve ono što od njega očekujemo. Iz tog razloga za izbor hardverskih komponenti za slaganje računalnog sustava odlučuje se za komponente proizvedene od poznatih i provjerenih firmi koje garantiraju za svoju opremu u velikom broju sati rada do pojave moguće tehničke greške (MTBF). Drugi segment pouzdanosti rada je i softverski dio sustava, koji bez dobre konfiguracije i održavanja može stvoriti velikih problema pristupu samog sustava, a u najgorem scenariju i gubitak podataka.

Pouzdanost operativnog rada sustava se svodi na dva problema i to:

- Dijagnosticiranje grešaka
- Ispravljanje i obnavljanje procesa i podataka

Zaštita računalnih sustava je element sigurnosti koji možemo definirati kao onemogućavanje slučajnog ili namjernog otkrivanja i korištenja podataka od neovlaštenih osoba kao i njihovo neovlašteno mijenjanje ili brisanje istih. Zaštita je vrlo kompleksan problem jer je sačinjavaju različiti činioci. Sustav zaštite treba funkcionirati u svim fazama djelovanja računalnog sustava, počevši od njegovog projektiranja, nabavke opreme, izbora lokacije smještaja opreme, izbora osoblja i tokom operativnog

rada izvedenog računalnog sustava. Pored zaštite od opasnosti kao što su požar, poplava, krađa, zagađenost i drugo, posebna pažnja se posvećuje tajnosti.

Objekt zaštite tajnosti podataka je sadržaj određenih slogova, kompletnih datoteka i banaka podataka. Potreba zaštite tajnosti je osiguranje povjerljivih sadržaja podataka koji je na nivou društva propisan zakonom, a na nivou poduzeća posebnim aktima poduzeća.

Objekt zaštite podataka je fizička egzistencija pojedinih podataka ili čak cijelih banki podataka, koja je osigurana fizičkom postojanošću slogova, čime se osigurava pouzdana obrada i korištenje podataka. Za ostvarenje tog cilja potrebno je zaštititi sve komponente računalnog sustava, od hardware-a, software-a, kadrova do podataka i organizacije.

Zaštita je čitav niz metoda usmjerenih cilju zaštite informacijskih sadržaja i njihovog neautoriziranog korištenja. Zaštitom osiguravamo informacijski sadržaj od gubitka, uništenja ili nedozvoljenog korištenja. Mora biti cjelovito provedena tj. U svim segmentima računalnog sustava. Najprije treba izvršiti procjenu rizika o kojoj će zavisiti od čega treba štititi računalni sustav i kojim metodama.

Troškovi zaštite moraju biti niži od troškova gubitaka podataka.

2.4. Zakonska obaveza čuvanja i zaštite podataka i informacija

Zakonom se utvrđuje vrijeme čuvanja pojedinih dokumenta koji nastaju u okviru te službe.

Pojedini se dokumenti čuvaju:

- trajno, (godišnji i konačni obračun osobnih dohodaka radnika, mjesečne isplatne liste za radnike kada se ne raspolaže s godišnjim obračunom)
- najmanje deset godina, (glavna knjiga i dnevnik knjiženja)
- pet godina, (pomoćne knjige, polugodišnji i drugi periodični obračuni i knjigovodstvene isprave na temelju kojih su vršena knjiženja)
- tri godine, (isprave koje se odnose na platni promet; odnosi se na organizacije koje su ovlaštene za obavljanje platnog prometa)
- dvije godine, (prodajni i kontrolni blokovi, pomoćni obrasci i slična dokumentacija).

3. SIGURNOST RAČUNALNIH SUSTVA

Fizička sigurnost opisuje mjere koje sprječavaju neovlašten pristup resursima ili informacijama pohranjenim na fizičkim medijima. Radi se o skupu smjernica za dizajniranje strukture koja je otporna na razne zlonamjerne radnje, a može uključivati jednostavnu primjenu zaključavanja vrata ili zapošljavanje zaštitara.

Fizička sigurnost je najosnovniji aspekt zaštite, a obuhvaća kontrolu zaštite prostorija, postrojenja, zgrada i druge imovine. Primjena fizičke sigurnosti podrazumijeva proces uporabe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara. U osnovi, fizička sigurnost odnosi se na sprječavanje oštećenja bilo kojeg dijela nekretnina, postrojenja, ureda, objekata ili zgrada.

Također, ona doprinosi zaštiti ljudi i informacija, iako se na te skupine primjenjuju i druge sofisticirane mjere zaštite. Prema tome, fizička sigurnost čini dio sveukupne sigurnosti informacijskog sustava kao osnova na kojoj su sve sigurnosne mjere utemeljene.

Mjere koje uključuje fizička sigurnost, a služe za zaštitu osoblja, opreme i imovine, mogu se podijeliti na:

- Pasivne mjere – efektivna uporaba arhitekture, okoliša i osvjetljenja za postizanje bolje sigurnosti kroz olakšanu detekciju upada ili potencijalnih prijetnji.
- Aktivne mjere – uključuju upotrebu poznatih sustava i tehnika dizajniranih za detekciju i reakciju na prijetnje.

3.1. Aspekti fizičke sigurnosti

Fizička sigurnost može se promatrati preko tri aspekta:

1. Fizički aspekt – mjere poduzete da bi se osigurala imovina (npr. Zapošljavanje zaštitara).
2. Tehnički aspekt – mjere poduzete za osiguravanje usluga i elemenata koji služe kao podrška informacijskim tehnologijama (npr. sigurnost sobe s poslužiteljima).
3. Operacijski apekt – općenite sigurnosne mjere koje se provode prije izvođenja neke operacije (npr. analiziranje prijetnji ili aktivnosti).

Bez obzira na gledište, svi aspekti imaju zajedničke ciljeve:

- spriječiti bilo kakav neautorizirani pristup računalnom sustavu,
- spriječiti krađu podataka s računalnih sustava,
- zaštititi integritet podataka pohranjenih na računalu i
- spriječiti gubitak ili oštećenje podataka uslijed bilo kakvih nepogoda ili nesreća.

3.2. Uloga fizičke sigurnosti

Fizička zaštita se koristi kako bi se osiguralo da samo ovlaštene osobe imaju pristup nekretninama i informacijskom sustavu. Primijenjene mjere zaštite moraju biti prilagođene radnom okruženju, a ovise o sljedećim faktorima:

1. Koju imovinu treba zaštititi?
2. Gdje je smještena imovina koju treba zaštititi?
3. Koliku vrijednost ima imovina koju treba zaštititi?
4. Koje ranjivosti, prijetnje ili rizici prijete imovini?

Primjena odgovarajuće razine zaštite u svakom okruženju zahtjeva dizajniranje fizičke sigurnosti u procesu izgradnje i konstrukcije. Kako bi se postigla najbolja razina zaštite, arhitekti i sigurnosni stručnjaci trebali bi zajedno proučiti sve aspekte zaštite primjenjive na neku radnu okolinu. Ovakav oblik planiranja pomaže pri stvaranju optimalne sigurnosti uz najmanje troškove (jer se time zaobilaze brojni sigurnosni problemi).

Sigurnosni problemi koji se jave kao posljedica pogreške u fazi dizajniranja i konstrukcije obično zahtijevaju puno napora za otklanjanje te uzrokuju velike novčane izdatke. Jedno od rješenja u tom slučaju je primjena dodatnih mjera zaštite koje nisu prvotno planirane. Ukoliko se fizička sigurnost ne primjeni u početnoj fazi, potrebno je adresirati sigurnosne probleme prije puštanja postrojenja u rad.

Najbolja praksa primjene fizičke sigurnosti je u slojevitom pristupu, jer ne postoji niti jedna sigurnosna kontrola koja će u potpunosti zadovoljiti sve zahtjeve. Slojevitu primjenu kontrola potrebno je implementirati od unutarnjih do vanjskih granica informacijskog sustava kako je vidljivo na Slika 5.

Vanjski slojevi zaštite ovise o tipu nekretnine i lokaciji. Na primjer, objekt smješten u gradu može imati samo zid ili ogradu oko objekta, dok imovina smještena

u industrijskom području može imati velika zelena područja, parkirališta i sl. u svojoj okolini. Kod drugog tipa objekta, okolina stvara dodatnu prepreku za fizički pristup.

Za razliku od vanjskih slojeva, unutarnji slojevi zaštite uključuju mjere primijenjene u uredima, na ulazu u objekt i sl. Usmjeravaju se na zaštitu svih unutarnjih dijelova objekata i imovine.

Slika 5. Slojevita fizička zaštita (izvor:https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-06-304.pdf)

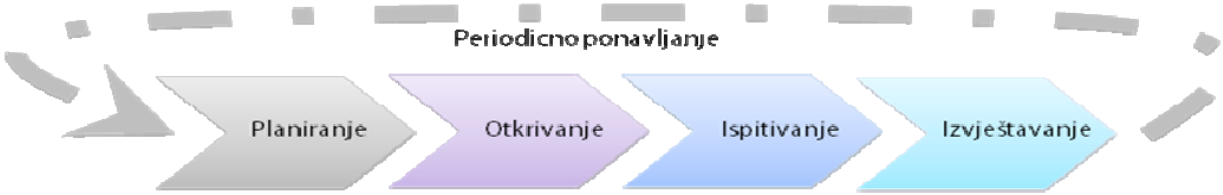
3.3. Procjena fizičke sigurnosti

Procjena fizičke sigurnosti vrlo je važna za svaku organizaciju i to u svakom trenutku. Ona ukazuje na stupanj pripremljenosti na prijetnje fizičkoj sigurnosti te pokazuje kolike bi gubitke mogla pojedina prijetnja uzrokovati.

U procjenu fizičke sigurnosti uključeno je:

- ocjenjivanje stupnja sigurnosti lokacije,
- ispitivanje procedura za zaposlenike i njihove svijesti o problemima,
- procjena sigurnosti sve imovine te
- ocjena sigurnosti zaposlenika.

Postupak procjene fizičke sigurnosti sastoji se od četiri faze prikazane na Slika 6. Prva faza podrazumijeva planiranje i tu se definira raspon procjene, uloge te cilj. Nakon planiranja slijedi faza otkrivanja u kojoj se prikuplja što je više moguće informacija. Treća faza je testiranje, a uključuje provođenje „penetracijskih ispitivanja“ izvođenjem neke vrsta napada socijalnim inženjeringom. Nakon provođenja ovih faza slijedi posljednja faza u kojoj se stvaraju izvještaji o razini fizičke sigurnosti. Opisane faze slikovito su prikazane na Slika 6. Postupak procjene fizičke sigurnosti treba obavljati periodično jer se rizici i prijetnje mogu mijenjati tokom vremena. Prema tome, ovaj je postupak vrlo važan jer može pomoći pri otkrivanju novih prijetnji i ranjivosti. [2]



Slika 6. Koraci procjene sigurnosti (izvor:https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-06-304.pdf)

[2] https://www.cert.hr/wpcontent/uploads/2019/04/NCERT-PUBDOC-2010-06-304.pdf

4. PRIJETNJE FIZIČKOJ SIGURNOSTI

4.1. Prirodne nepogode

Prirodne prijetnje jedne su od najprisutnijih opasnosti za fizičku sigurnost na koje čovjek ne može utjecati. Ipak, postoje određene mjere kojima je moguće smanjiti njihov štetan učinak na sigurnost informacijskog sustava.

U skupinu prirodnih prijetnji spadaju:

- meteorološke nepogode – uključuju sve atmosferske nepogode poput raznih padalina (kiša, snijeg), vjetra, oluje, jako visokih i niskih temperatura i sl. Neke od posljedica ovih nepogoda na informacijski sustav su gubitak ili degradacija komunikacija te uništenje uređaja (a samim time i informacija).
- geofizičke nepogode – podrazumijevaju potrese i vulkanske aktivnosti, a mogu izazvati niz drugih nepogoda poput požara, poplava, ispuštanja plina ili otrovnih kemikalija, prekida napajanja i sl. Kao osnovni učinci ovih prijetnji javljaju se mogućnosti uništenja ili oštećenja uređaja što može rezultirati gubitkom podataka, prekidom rada sustava i velikim materijalnim gubicima.
- sezonski fenomeni – uključuju nepogode vezane uz neko razdoblje poput vremenskih ekstrema, šumskih požara ili uragana, a mogu dovesti do gubitka ili degradacije mrežnih komunikacija te uništenja uređaja.
- astrofizički fenomeni – podrazumijevaju sunčane fenomene i meteore koji mogu uzrokovati gubitak ili degradaciju satelitskih veza.
- biološke prijetnje – razne bolesti koje mogu uzrokovati smanjenje broja sposobne radne snage.

Prirodne prijetnje mogu dovesti do ogromnih materijalnih gubitaka i prouzročiti veliku štetu kako je vidljivo i na Slika 3. Ne postoje nikakve metode zaštite koje bi spriječile pojavu prirodnih nepogoda. Ipak, moguće je poduzeti mjere koje će omogućiti nastavak neprekidnog rada informacijskog sustava i spriječiti gubitak informacija potrebnih za poslovanje. Takvi postupci umanjuju nepovoljne posljedice koje donose neke od opisanih prirodnih nepogoda.

4.1. Ljudske prijetnje

Zaposlenici su jedan od osnovnih rizika svake organizacije jer unose veliki raspon prijetnji sigurnosti informacijskog sustava. Neke od prijetnji, prikazane na Slika 7, koje uzrokuju zaposlenici su:

- Neposlušnost – jedna od prijetnji ove skupine javlja se uslijed neposlušnosti zaposlenika što može dovesti do prosvjeda ili štrajka. Posljedice takve situacije mogu biti oštećenje imovine ili uređaja te ozljeđivanje samih zaposlenika.
- Otkrivanje osjetljivih podataka – zaposlenici također mogu nanijeti druge oblike šteta poput otkrivanja osjetljivih podataka zbog nepravilnog rukovanja ili nerazumijevanja/nepostojanja sigurnosne politike.
- Sabotaža – svaka organizacija trebala bi uvesti i zaštitu od sabotaže ili namjernog narušavanja rada sustava i ispravnosti uređaja.
- Nenamjerno oštećenje imovine – nepravilno rukovanje može dovesti do oštećenja uređaja ili drugih dijelova imovine. Kako bi se to spriječilo, zaposlenike treba pravilno educirati i upozoriti na posljedice nepravilnog korištenja.
- Zlouporaba ovlasti – zaposlenicima treba jasno definirati uloge te objasniti prava i posljedice njihovog nepridržavanja. Zlouporaba ovlasti može se odraziti u obliku prekomjernog korištenja imovine organizacije ili njenog iznošenja izvan prostora za koji je namijenjena.
- Neovlašten pristup podacima ili imovini – zaposlenicima treba pravilno definirati prava pristupa kako ne bi došli do povjerljivih podataka. Ukoliko zaposlenici rade s nekim povjerljivim podacima ili dijelovima sustava potrebno je napraviti ugovore o povjerenju.
- Krađa – zaposlenici koji imaju pristup imovini organizacije mogu prisvojiti neke dijelove ili uređaje.

Slika 7. Ljudske prijetnje (izvor:https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-06-304.pdf)

Dosta opisanih prijetnji dolazi ne samo od zaposlenika, već od korisnika, klijenata, poslovnih partnera, dostavljača te ostalih osoba koje imaju doticaja s imovinom i podacima organizacije. Svaka osoba koja na neki način dolazi u kontakt s poslovanjem ili imovinom organizacije može uzrokovati nenamjerno oštećenje imovine. Ipak, organizacije često ulažu velike napore i resurse u zaštitu od namjernog uništavanja, krađe dobara i podataka, sabotaže, terorizma, špijunaže i sl. Ljudski faktor čini ključnu ulogu u postizanju sigurnosti, a kako bi se ostvarila zaštita od navedenih prijetnji potrebno je brojne mjere implementirati i na samoj fizičkoj razini.

4.3. Socijalni inženjering

Postoji cijela skupina napada usmjerena na dobivanje pristupa računalnom sustavu iskorištavanjem ljudskih ranjivosti poput nemarnosti ili lakog povjerenja. Cilj tih napada je pridobiti povjerenje žrtve kako bi se ostvarila krađa identiteta ili podataka te izveo upad u mrežu/sustav. Socijalni inženjer može biti bilo tko, od hakera, špijuna, nezadovoljnih zaposlenika do prodavača i vladinih službenika.

Napadi temeljeni na socijalnom inženjeringu, prikazani na Slika 8, mogu se izvesti:

- oponašanjem dostavljača ili nekih službenih osoba kako bi se ostvario pristup sustavu,
- lažnim predstavljanjem u komunikaciji preko telefona (npr. kao osoba zaposlena u tehničkoj podršci),
- uvjeravanjem osoba da će dobiti nagradu ukoliko obave neki zadatak,
- prikupljanjem informacija o navikama zaposlenika kako bi se iste mogle iskoristiti kao njihove slabosti te
- „izvlačenjem“ informacija od zaposlenika (npr. podataka za pristup).

Slika 8. Ljudske prijetnje (izvor:https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-06-304.pdf)

Općenito, napadi su uspješniji ako ne postoji definirana sigurnosna politika te nije provedena edukacija zaposlenika o opisanim opasnostima. Ukoliko su uspješno izvedeni, mogu uzrokovati velike gubitke za neku organizaciju poput otkrivanja osjetljivih podataka o zaposlenicima, partnerima i kupcima, zatim gubitka nacrta i planova za nova poslovanja i proizvode i sl.

Napadi socijalnog inženjeringa predstavljaju veliku prijetnju fizičkoj sigurnosti, ali njihov utjecaj može biti smanjen odgovarajućim mjerama.

5. TEHNIČKA ZAŠTITA RAČUNALNIH SUSTAVA

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 sprječavanje protupravnih radnji usmjerenih prema štićenim osobama ili imovini kao što su:

- protuprepadno djelovanje
- protuprovalno djelovanje
- protusabotažno djelovanje

Protuprepadno djelovanje je preventivni korak u zaštiti nekog objekta jer njime otkrivamo provalnika i pokušavamo ga odvratiti sa štićenog prostora. Taj je prostor ujedno i najzahtjevniji zbog izloženosti atmosferskim utjecajima, a prostor na kojemu je potrebno detektirati pokušaj provale mjeri se u stotinama metara. Zato se od opreme za detekciju očekuje velika pouzdanost i mala osjetljivost na vanjske utjecaje. Ovakvi detektori se najčešće se integriraju s rasvjetom kako bi upozorili provalnike da su uočeni te se ujedno aktivira i snimanje događaja putem lokalnog videonadzora.
Kod protuprovalnog djelovanja najvažniju ulogu imaju razni detektori za vanjsku i unutrašnju zaštitu otvora i prolaza koji predstavljaju potencijalno mjesto neželjenog ulaza u objekt, jer o detektorima ovisi razina zaštite objekta i njena obuhvatnost.
Za protuprovalu zaštićuju se svi vanjski rubovi (perimetri) objekta – vrata i prozori, pri kojoj se provalnici detektiraju već pri samom pokušaju ulaska u štićeni objekt.
S obzirom na način detekcije detektore možemo podijeliti na:

- prostorne detektore kretanja
- detektore vibracije i loma stakla
- kontakte za detekciju otvaranja

Kod protusabotažnog djelovanja pokušavamo spriječiti bilo kakav utjecaj, fizički ili programski, na sigurnosnu opremu. Tokom fizičkog napada najčešće se pokušava onesposobiti: videonadzor (zakretanje kamere radi promjene kuta snimanja, defokusirati ili zamagliti objektiv kamere i sl.), alarmne sirene ili neke od ugrađenih

detektora. Što se tiče zaštite od programskog napada većina baznih jedinica imaju ugrađene algoritme za prepoznavanje napada i njihovu dojavu.

5.1. Šest stupnjeva provedbe tehničke zaštite

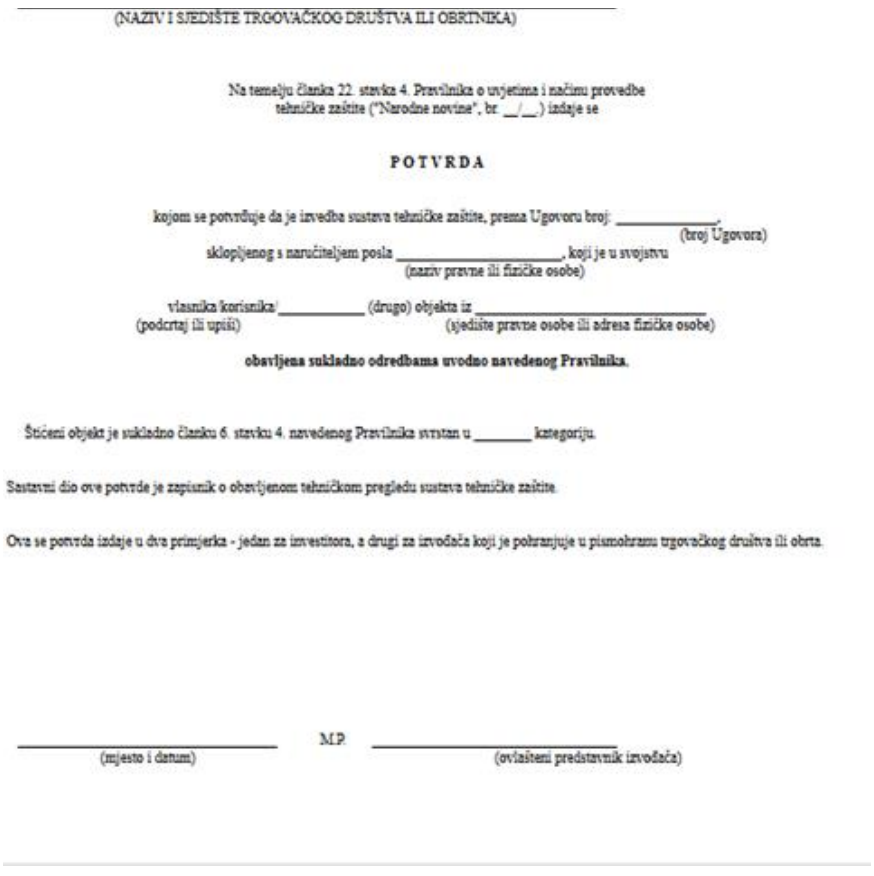
Priznata pravila u provedbi tehničke zaštite, su odgovarajuće hrvatske norme, a u nedostatku hrvatskih normi primjenjuju se odgovarajuće europske odnosno međunarodne norme (EN, IEC, ISO), odnosno druge specijalizirane norme te prihvaćena pravila struke. [1]

Pravne i fizičke osobe registrirane za obavljanje poslova tehničke zaštite štićeni objekt kategoriziraju u jednu od šest (6) kategorija koje sadrže obvezatne mjere zaštite:

1. NAJVIŠI STUPANJ ZAŠTITE koji predviđa:
    - mehaničku i tehničku zaštitu kojom se signalizira neovlašten ulazak u štićeni prostor i dojavljuje se na CDS (Centralni Dojavni Sustav)
    - tehničku zaštitu kojom se prati kretanje u štićenome prostoru i pojedinačno štićenim prostorijama (kontrola prolaza i videonadzor) uz video zapis
    - zaštitu pojedinačnih vrijednosti pomoću specijalnih trezora, blagajni
    - 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
2. 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 (1) lokalnim nadzornim mjestom i sustavom veze sa CDS-om
3. 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

4. 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
5. NIŽI STUPANJ ZAŠTITE koji predviđa:
   - mehaničku i tehničku zaštitu kojom se na licu mjesta zvučno ili svjetlosno signalizira neovlašten ulazak u štićeni prostor
6. MINIMUM ZAŠTITE koji predviđa:
   - mehaničku zaštitu bez uporabe elektroničkih naprava
   - obične cilindarske brave
   - obične ograde bez tehničkih elemenata (osim za stanove)[3]



_____
(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

POTVRDA

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)

Slika 9. Slika potvrde izvedbe radova i u koju kategoriju (stupanj) je svrstana izvedena tehnička zaštita (izvor: http://www.propisi.hr/print.php?id=3980)

[3] http://www.propisi.hr/print.php?id=3980

5.2. Ostale zakonske regulative za provedbu tehničke zaštite

5.2.1. Sigurnosni elaborat

Na temelju izrađene prosudbe i svrstavanja objekta u jednu od šest kategorija navedene zaštite, izrađuje se sigurnosni elaborat. Njime se utvrđuje optimalna razina tehničke zaštite, integralne zaštite sa svim tehnološkim sustavima u objektu.

Sigurnosnim elaboratom se utvrđuju: zahtjevi koje moraju ispuniti sustavi koji nisu sustavi tehničke zaštite, ali utječu na sigurnost objekta i pouzdan rad tehničke zaštite (sustavi napajanja električnom energijom, rasvjeta i sl.), građevni i slični zahtjevi od značaja za pravilan i pouzdan rad tehničke zaštite(niveliranje terena, sigurnosni razmaci, uređenje okoliša i sl.) [1]. Da bi se kvalitetno izradila prosudba ugroženosti i sigurnosni elaborat veoma je bitno u obzir uzeti sljedeće činjenice:

- zahtjeve naručitelja
- snimku postojećeg stanja objekta
- točnu lokaciju objekta (blizina prometnica i okolnih objekta)
- karakteristike objekta
- namjena objekta
- ukoliko se radi o poslovnoj građevini, radno vrijeme te broj zaposlenih djelatnika sa strukturom zaposlenika
- oprema i vrijednosti u objektu
- analiza moguće opasnosti

Na temelju izrađenog sigurnosnog elaborata i posebnih zahtjeva korisnika objekta izrađuje se projektni zadatak.[4]

5.3.1. Projektni zadatak

Projektnim zadatkom utvrđuju se sve veličine (parametri) potrebni za izradbu projekta sustava tehničke zaštite, a osobito: vrsta tehničke zaštite, smještaj centra tehničke zaštite, smještaj opreme i način polaganja instalacija.

Projektiranje sustava tehničke zaštite obuhvaća:

- odabir vrste i opsega tehničke zaštite

[4] http://www.poretti.hr/projektiranje-i-konzalting/izrada-elaborata/

- odabir uređaja i opreme
- razradu koncepcije tehničke zaštite
- izradbu projektne dokumentacije

Snimka postojećeg stanja štićenog objekta i analiza problema s ocjenom, prosudba ugroženosti, sigurnosni elaborat i projektni zadatak, čine sastavni dio projekta sustava tehničke zaštite.[5]

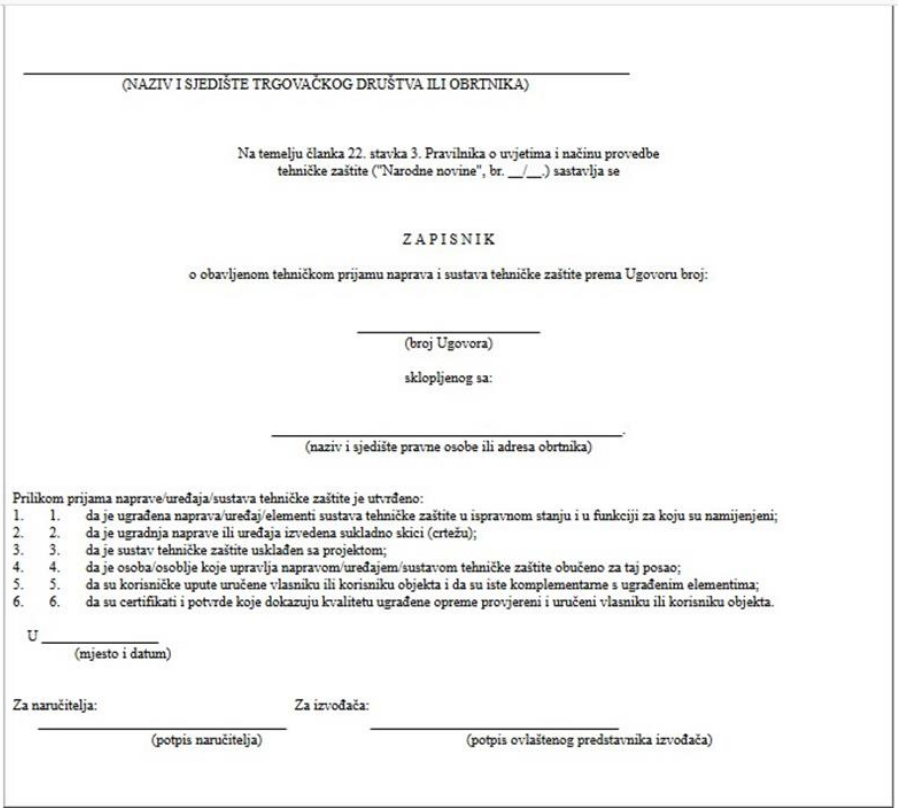
5.2.3. Izvedba tehničke zaštite

Nakon izrađene tehničke dokumentacije projekta, dolazi se do izvedbe radova tehničke zaštite kod koje se podrazumijeva sljedeće:

- izvedbu instalacija
- ugradnju uređaja i opreme
- programiranje, parametriranje i ispitivanje sustava tehničke zaštite te njegovo puštanje u probni rad
- verifikacija uređaja i opreme, odnosno sustava i tehnički prijem
- izradu uputa za rukovanje
- obuku osoblja

Nakon izvršenih radova i svih instalacija potrebno je izvršiti provjere tehničke zaštite: ispravnosti i funkcionalnosti svih uređaja i opreme, usklađenosti sustava tehničke zaštite sa projektom, obučenosti osoblja. korisničkih uputstava za rukovanje, dokaza kvalitete ugrađene opreme.

[5] http://www.propisi.hr/print.php?id=3980



_____
(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

ZAPISNIK

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

Slika 10. Zapisnik o izvedenim radovima i potvrđenosti o ispravnosti opreme i instalacija i rada sustava tehničke zaštite
(izvor:http://www.propisi.hr/print.php?id=3980)

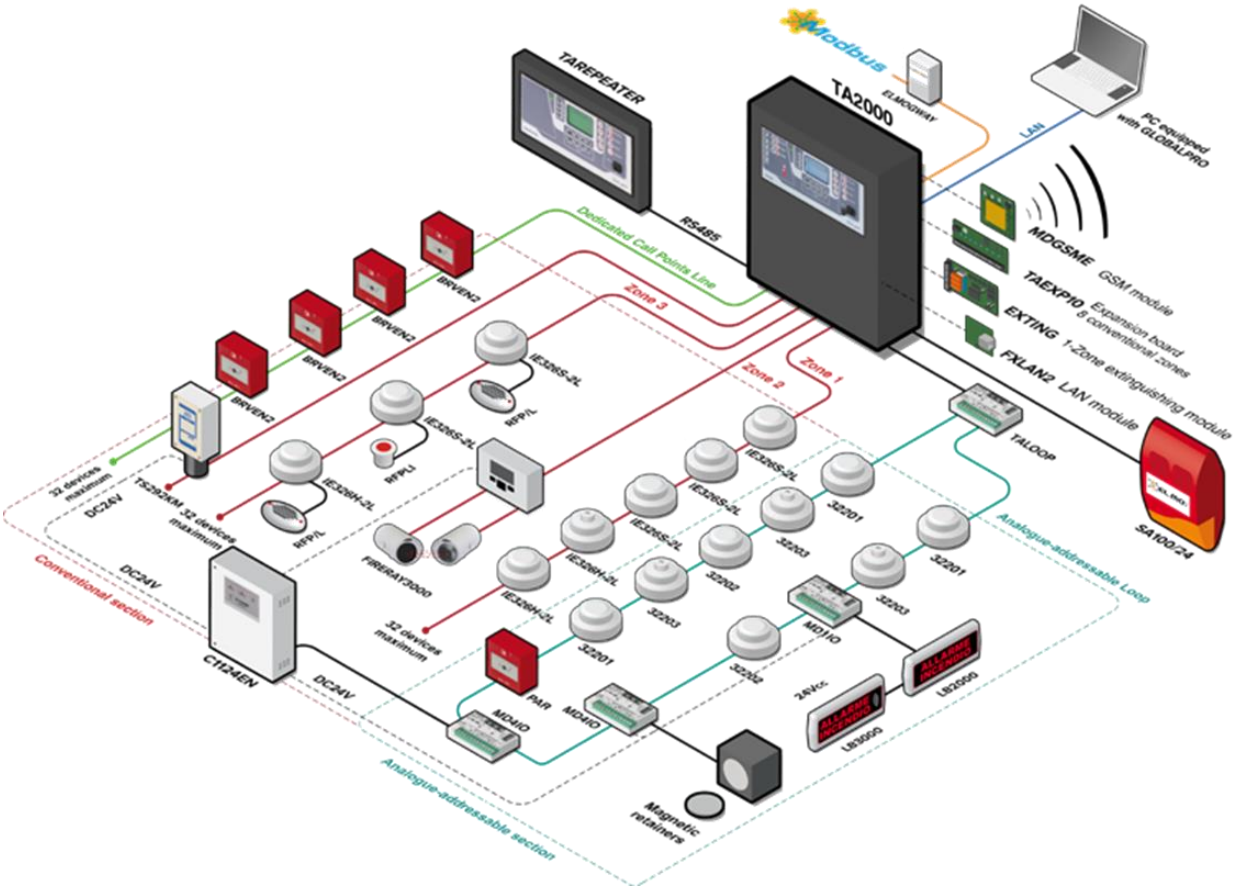
5.3. Tehnički elementi za provedbu sustava tehničke zaštite

Nakon opisanih općenitih zakonskih regulativa za provedbu tehničke zaštite, u ovom poglavlju biti će opisani tehnički elementi koji se koriste u sustavima tehničke zaštite, odnosno razne elektroničke elemente i njihove funkcije.

5.3.1 Vatrodojava

Vatrodojava ili dojava požara je elektronički sustav inteligentnih kontrolera, centrale, upravljanja, ulazno-izlaznih i izvršnih elemenata koji samostalno očitavaju situaciju štićenog objekta i u svakom trenutku javljaju situaciju prema kojoj izvršavaju zadane funkcije tj. dojavljuju stanje požara, porast temperature i izvršavaju prema

procjeni kontrolu otvaranja ili zatvaranja vrata, prozora, kupola, dizala i samo gašenje građevine.[6]



Slika 11. Predodžba alarmnog sustava za dojavu požara (izvor: http://elmospa-zoo.s3.amazonaws.com/Brochure_di_gamma/Antincendio/Tacora_D.23.1218.5_EN_web.pdf)

Velike građevine često imaju potrebu za centralnom integracijom sustava vatrodojave sa sustavima tehničke zaštite (videonadzor, kontrola pristupa i sl.)

5.3.1.1. Vrste sustava vatrodojave

Osnovni sustav vatrodojave se sastoji od sljedećih komponenata:

- vatrodojavna centrala (glavna inteligentna komponenta sustava vatrodojave koja prati stanje ulaznih elemenata, detektora i izvršava funkciju dojave i upravljanja izvršnim elementima)

[6] http://vatrodojava.hr/strucni-clanci/sigurnost/kako-funkcionira-vatrodojava

- javljači požara (optički, termički, laserski, ručni, sonde)
- signalizacija (zvučna, svjetlosna, evakuacijski tabloi)
- izvršni elementi (moduli za upravljanje sustavima za gašenje ili usporavanje širenja požara koji se integriraju u sustav vatrodojave)

Sama vatrodojava podrazumijeva širok spektar sustava zavisno o vrsti zahtjeva korisnika i same građevine:

1. Samostojeći (eng. Stand-alone) uređaji
   - samostojeći detektori porasta temperature ili dima koje korisnik sam može ugraditi (takvi detektori najčešće rade na bateriju i imaju zvučnu i svjetlosnu signalizaciju)
   - namjena je zaštita stana ili kuće manjih kvadratura koja će zaštititi korisnika od požara dok je korisnik u objektu. Statistika kaže da je najveći broj nehotično izazvanih požara kod kuće u noći zbog kvara uređaja ili nepažnje osoba
2. Konvencionalni sustavi
   - glavna karakteristika konvencionalnih sustava je ta da se svi elementi detekcije žičano ili bežično vežu na vatrodojavnu centralu koja prati stanje i javlja opasnost
   - sustavi vatrodojave koji uz zvučnu i svjetlosnu signalizaciju javljaju detekciju požara odgovornoj osobi (vatrogasci ili korisnik) putem telefonske, IP ili GSM veze
3. Analogno adresabilni sustavi dojave požara
   - sustavi vatrodojave koji uz zvučnu i svjetlosnu signalizaciju javljaju točnu lokaciju detekcije požara unutar veće građevine odgovornoj osobi (vatrogascima ili korisniku) putem telefonske, IP ili GSM veze
   - glavna karakteristika analogno-adresabilnih sustava vatrodojave je profesionalna zaštita ljudi i imovine u građevinama specijalne namjene i velikim građevinskim kompleksima. Pomoću detekcije mikrolokacije dima ili požara u velikom kompleksu, sustav može osigurati preciznu dojavu vatrogasnoj postrojbi ili pokrenuti sustav gašenja te izbjeći veliku vatrenu stihiju

- namjena analogno-adresabilnih sustava vatrodojave se odnosi na srednje građevine specijalnih namjena (kemijska obrada, proizvodnja), javne ustanove, velike građevine i industriju.[7]

5.3.1.2. Vrste i načini detektora požara

Osnova svakog alarmnog sustava za dojavu požara jesu detektori, koji mogu biti sofisticirani inteligentni uređaji za dojavu dima ili vatre ili jednostavnih ručno upravljane sklopke koje aktiviraju zvučnu signalizaciju. No sve ih možemo raspodijeliti u pet kategorija:

- detektori topline
- detektori dima
- detektori ugljičnog monoksida
- multi-sensor detektori
- ručno upravljani
-

Navedene vrste detektora spajaju se u razne kombinacije sustava (konvencionale ili analogno adresabilne sustave), a svima im je zajednička kontrolna jedinica koja prima signale od detektora i uključuje obavještajnu signalizaciju (zvučnu, svjetlosnu ili kombinacija obje).[8]

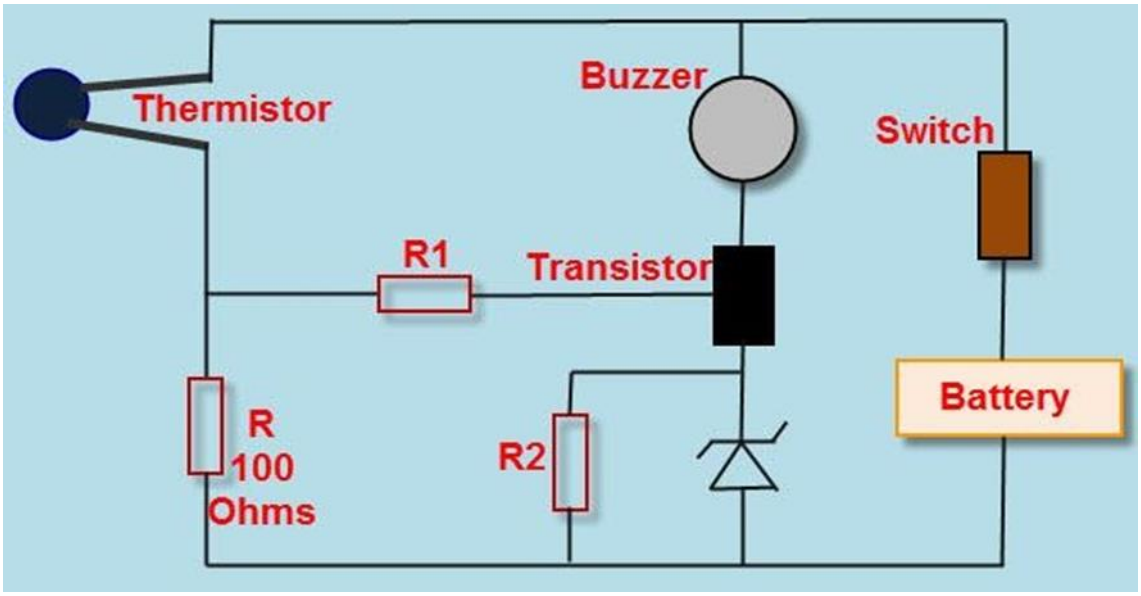
- **Detektori topline**

Klasificirani su u dvije kategorije. Prva kategorija su detektori topline sa fiksnom temperaturom (eng. ˝fixed temperature heat detector“), a druga kategorija su detektori topline sa ocjenom porasta temperature (eng. ˝rate of rise heat detector“).

Detektori sa fiksnom temperaturom su najčešće korišteni detektori topline. Kada dođe do porasta temperature dolazi do prijelaza eutektičke točke eutektičke legure iz čvrstog u tekuće stanje koji je ujedno i osjetilni element. Sa svojom promjenom agregatnog stanja pomiče se metalna pločica koja preko opruge zatvara električni krug i aktivira signalizaciju.

[7] http://vatrodojava.hr/strucni-clanci/sigurnost/kako-funkcionira-vatrodojava
[8] https://realpars.com/fire-alarm-system

Detektori s ocjenom porasta temperature funkcioniraju tako da mjere brzinu promjene temperature u vremenskom intervalu koji obično iznosi od 6.7-8.3[°C/min]. Osjetilni elementi su dva termopara ili termistora. Jedan termistor se koristi za nadziranje prijenosa topline zračenjem, a drugi termistor služi za nadziranje ambijentalne temperature. Detektor će dati izlazni signal ako se promjeni otpor prvog termistora zbog povećanja temperature u odnosu na drugi termistor.[9]



Slika 12. Predodžba jednostavne sheme dojave požara sa jednim termistorom (izvor: https://www.elprocus.com/heat-detector-circuit-working)

Na slici 12. prikazan je jednostavan krug detektora topline sa jednim termistorom koji se može upotrijebiti kao senzor topline. U ovom električnom krugu detektora topline stvara se djelitelj napona sa serijskim spojem termistora i otporom 100 Ohma. Ako se koristi N.T.C. (koeficijent negativne temperature) termistor, otpor termistora se smanjuje nakon zagrijavanja. Dakle, više struje teče kroz krug djelitelja napona koji tvori termistor i otpor 100 Ohma. Stoga se pojavljuje više napona na spoju termistora i otpornika. Uzmimo u obzir da termistor ima 110 Ohma, a nakon zagrijavanja njegova vrijednost otpora postaje 90 Ohma. Ulazno-izlazni odnos za ovaj sustav kruga detektora topline ima oblik omjera izlaznog napona i ulaznog napona koji je dan u konceptu djelitelja napona u ovom konkretnom konceptu. Na kraju, izlazni napon se primjenjuje na prikazani NPN tranzistor u krugu kroz otpornik. Zener dioda

[9] https://www.elprocus.com/heat-detector-circuit-working

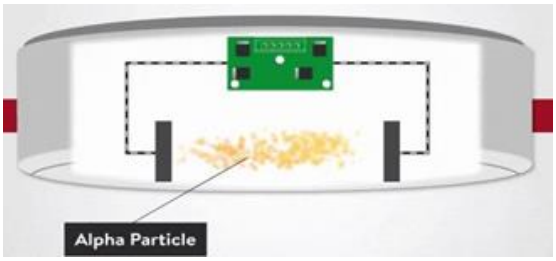
se koristi za održavanje napona emitera na 4,7V, koji se može koristiti usporedno. Ako je osnovni napon veći od napona emitera, tada tranzistor započinje provođenje. To je zato što i tranzistor i zujalica, koja se koristi za proizvodnju zvuka, dobivaju više od 4.7V baze napona i povezani su tako da zatvaraju krug detektora topline.[10]

- **Detektori dima**

Postoje tri osnovna tipa detektora dima:

1. Ionizacijski detektor dima

Sastoji se od dvije komore. Prva komora služi kao referenca za kompenzaciju promjena u ambijentalnoj temperaturi, vlažnosti i tlaku. Druga komora sadrži radioaktivni izvor, obično alfa čestice, koje ioniziraju zrak prolazeći kroz komoru gdje prolazi struja između dvije elektrode. Kada dim uđe u komoru tok struje se smanji. To smanjenje struje služi za aktivaciju alarma.[11]

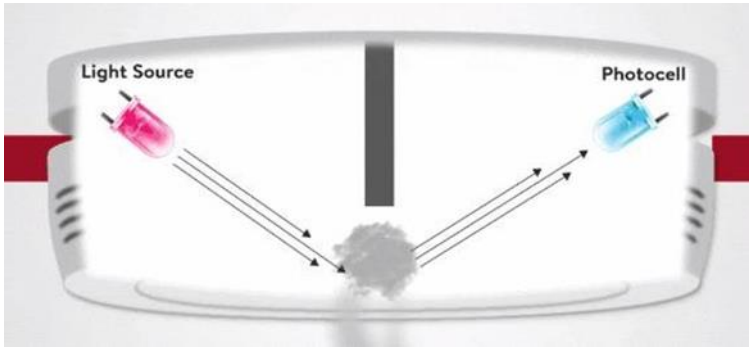


Slika 13. Predodžba jednostavne sheme dojave požara sa jednim termistorom (izvor: https://www.elprocus.com/heat-detector-circuit-working/)

2. Detektor dima sa principom raspršivanja svjetlosti

Za rad koristi Tyndallov efekt. Sastoji se od izvora i prijemnika svjetlosti koji su odvojeni zatamnjenom komorom tako da izvor svjetla ne pada na prijemnik. Kada dim uđe u komoru svjetlost se raspršuje i dio pada na prijemnik. Izlaz sa prijemnika se koristi za aktivaciju alarma.

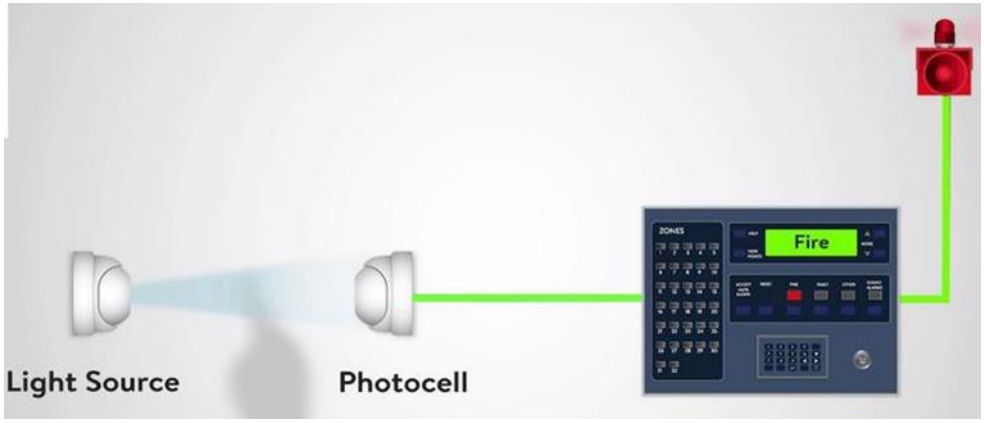
[10] https://www.elprocus.com/heat-detector-circuit-working
[11] https://realpars.com/fire-alarm-system



Slika 14. Predodžba rada detektora dima sa principom raspršivanja svijetlosti (izvor:https://realpars.com/fire-alarm-system)

3.) Detektor dima sa zatamnjenjem svjetlosti

Kod ovog detektora dim ometa svjetlosni snop između izvora i prijemnika. Prijemnik mjeri količinu svjetlosti koju prima. Razlika na izlazu iz prijemnika koristi se za aktivaciju alarma. Ova vrsta detekcije može se koristiti za zaštitu velikih područja s izvorom svjetlosti i prijemnika postavljenom na većoj udaljenosti (max. 100 metara).[12]



Slika 15. Predodžba rada detektora dima sa principom zatamnjenja svjetlosti (izvor:https://realpars.com/fire-alarm-system)

- **Detektori ugljičnog monoksida**

Elektronički uređaji koji se koriste za otkrivanje izbijanje požara mjerući količinu ugljičnog monoksida u zraku. U ovom slučaju, ti detektori nisu isti kao detektori ugljičnog monoksida koji se koriste u kući za zaštitu stanovnika od ugljičnog monoksida proizvedenog nepotpunim izgaranjem u uređajima kao što su plinski

[12] https://realpars.com/fire-alarm-system/

požari ili kotlovi. Detektori ugljičnog monoksida imaju elektrokemijsku ćeliju koja osjeća ugljični monoksid, ali ne i dim ili bilo koje druge proizvode izgaranja.

- **Multi-sensor detektori**

Multi senzorski detektori kombiniraju ulaze optičkih i toplinskih senzora i obrađuju ih sofisticiranim algoritmom ugrađenim u sklop detektora. Kad upravljačka ploča odradi ispitivanje, detektor vraća vrijednost koja se temelji na kombiniranim reakcijama optičkih i toplinskih senzora. Dizajnirane su da budu osjetljive na širok raspon požara.[13]

- **Ručno upravljani**

Ručno upravljani uređaj omogućuje osoblju da sami aktiviraju alarm razbijanjem osjetljivog lomljivog elementa na uređaju.

5.3.2. Kontrola pristupa

Kontrola pristupa je način ograničavanja pristupa nekom sustavu sa fizičkim ili virtualnim resursima koji je zastupljen u prvom, drugom i trećem stupnju provedbe tehničke zaštite. U sustavima kontrole pristupa, korisnici moraju pokazati akreditaciju prije nego im je dozvoljen pristup. U fizičkim sustavima, akreditacije mogu doći u raznim oblicima, ali najsigurnije su one koje se ne mogu prenijeti.

Postoje tri faktora koja se mogu koja se mogu koristiti za autentifikaciju:

- nešto što je poznato samo korisniku (šifra ili PIN kod)
- nešto što je dio korisnika (biometrijska očitanja prsta i sl.)
- nešto što pripada korisniku (ključevi ili ID kartica i sl.)

Kako ključevi ili kartica mogu biti ukradeni i neovlaštena osoba može pristupiti štićenom objektu, ovo i nije najbolje rješenje za zaštitu objekta tj. da bude ugrađeno kao jedina zaštita. Zato je najbolje koristiti kombinacije autentifikacija za što bolju zaštitu objekta (naprimjer koristiti karticu za pristup štićenom objektu i biometrijsko očitanje ili PIN kod za potvrdu identiteta). U ovom radu opisati ću dva najčešća

[13] https://realpars.com/fire-alarm-system/

načina kontrole pristupa koja se koriste u većini štićenih objekata, a to su : očitanje karticom/ privjescima koji koriste RFID tehnologiju i biometrijsko očitanje korisnika.[14]

5.3.2.1. RFID kao autentifikacija

RFID je kratica za ˝Radio Frekventnu Identifikaciju“ a koristi se u tehnologiji gdje se digitalni podatci, koji su spremljeni u RFID oznake (eng. ˝tag˝) očitavaju pomoću čitača koji koristi radio valove za očitanje podataka.
RFID sustav se sastoji od 3 dijela:

- antene ili zavojnice
- transceiver (odašiljač/prijemnik)(eng. ˝transmitter / receiver˝)
- transponder(odašiljač/odgovaratelj)(eng.˝transmitter / responder˝), i koristi se u dvije kombinacije:
- kombinacija je antene i transceivera koja se služi kao RFID čitač
- kombinacija je antene i transpondera i služi kao RFID oznaka.

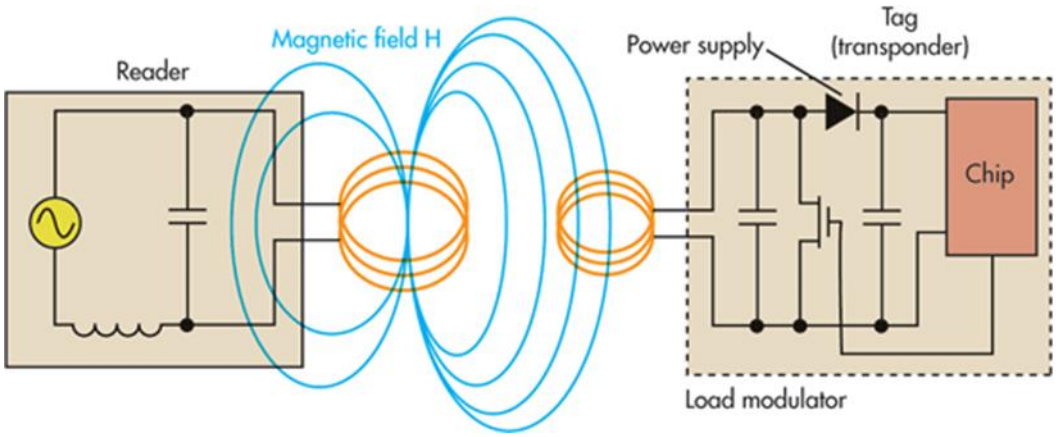
RFID Oznake se dijele u dvije kategorije:

- aktivne
- pasivne.

Aktivna oznaka ima unutarnji izvor napajanja koji koristi za generiranje signala kao odgovor na čitač. Mogu komunicirati na kilometarskim udaljenostima i koriste se većinom u navigacijskim sustavima i relativno je skupa izvedba.

Pasivna oznaka nema vlastiti izvor napajanja već koristi energiju koju daje čitač kako bi mogla dati odgovor. Ove oznake su jeftine i koriste se za robu široke potrošnje. Slika 16. prikazuje način rada pasivne oznake koji se zasniva na induktivnom uparivanju za očitavanje podataka.

[14] https://www.techopedia.com/definition/5831/access-control



Slika 16. Induktivno uparivanje za NF i VF krugove (izvor: https://www.electronicdesign.com/technologies/communications/article/21799760/design-opportunities-proliferate-as-rfid-gains-traction)

Za primjer kontrole pristupa izabran je model „REX K-1-B˝ u svrhu što boljeg protuprovalnog djelovanja i neovlaštenog ulaska u štićeni objekt. U slučaju računalnog sustava postavljen je na ulazu, a kontrola je preko pina ili kartice.

Slika 17. Kontrola pristupa „REX-K-1-B“ (izvor: https://kamir.hr/rex-k-1-b)

Neke tehničke specifikacije kontrole pristupa:

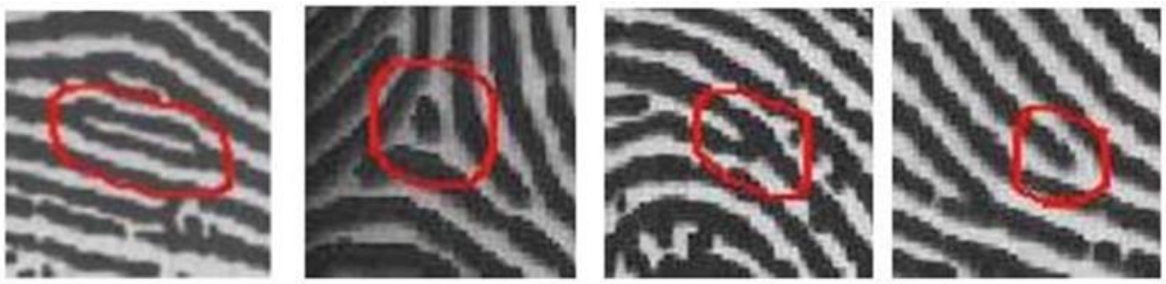
- Samostalni kontroler/čitač do 1000 korisnika/kartica/privjesaka, 10000 događaja
- RS485, tipkovnica
- Frekvencija 125kHz, domet za očitanje 10 cm
- Mogućnost izlaza Wiegand 26-bitLED (crveno/zeleno) i zvučna signalizacija promjene stanja

- Dimenzija kućišta: 58x120x15 mm, zaštita kućišta tamperom
- Napajanje 9 to 14V DC (preporuka Spider W5 ili Spider W40)
- Radna temperatura: -20 do +60°C, zaštita kućišta IP65
- Izlaz za el.bravu (500mA)[15]

5.3.2.2. Biometrisko očitanje prsta kao autentifikacija

Biometrijska očitanja i identifikacija prsta smatraju se danas jedan od najjednostavnijih i najpouzdanijih načina identifikacije, jer se biometrijske značajke čovjeka unikatne i nemogu se ukrasti. Neke od prednosti su: nema potrebe za nošenjem ključeva, znački i sličnih oznaka, otklanja rizik da neovlaštena osoba uđe u štićeni objekt koristeći upotrebom otuđene kartice.

Identifikacija otiscima papilarnih linija prstiju i dlanova temelji se na jedinstvenom rasporedu udubljenja i ispupčenja kože – dermatoglifa. Identifikacijske detaljne točke sastoje se od :



a) otoka b) točke c) bifurkacija d) kraj brazde

Slika 18. Detaljne točke od kojih se sastoji ljudski otisak prsta za skeniranje (izvor: https://hrcak.srce.hr/file/282537)

Za evidentiranje otiska prsta i njihovu usporedbu postoje na tržištu brojne metode (optička metoda, kapacitivna metoda, radijska metoda, metoda tlaka, mikro-elektro-mehanička metoda, toplinska metoda). Ovdje će se detaljnije opisati optička i kapacitivna metoda kao najčešće korištene metode u praksi.

[15] https://kamir.hr/rex-k-1-b

5.3.3. Sustav za protuprepadno i protuprovalno djelovanje

Svrha ovih uređaja i sustava je pravovremeno otkrivanje i signalizacija pokušaja provale u štićeni objekt. Sustavi protuprovalne, protuprepadne i vanjske zaštite uglavnom se izvode kao jedinstven sustav. Za protuprepadno djelovanje koriste se razni detektori pokreta za uočavanje neželjene osobe, razni sustavi videonadzora, a za protuprovalu magnetski kontakti na vratima i prozorima te razni senzori koji će biti detaljnije opisani u daljnjem tekstu.

5.3.3.1. Detektori pokreta

Detektor pokreta protuprovalnog sustava javlja alarmnom sustavu da se u prostoru štićenja nalazi toplo tijelo u pokretu. Osim u alarmnom sustavu koristi u sustavu videonadzora, a najčešće je prisutan u tehnologiji automatizirane rasvjete. Izvršna funkcija mu je detektirati toplo tijelo u pokretu te obrađeni podatak uputiti centrali koja će izvršiti funkciju alarmne dojave putem poziva i zvučnog i svjetlosnog signala na sireni. U integraciji s videonadzorom, detektor će aktivirati na snimaču snimanje kamere u kadru na koji je postavljen detektor.

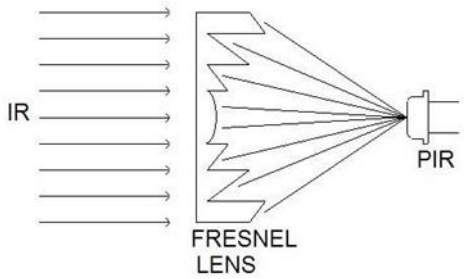
Osnovna svojstva detektora su: domet, širina pokrivenosti kadra (kut pokrivanja), osjetljivost, način povezivanja s centralom, zaštita i namjena.

PIR detektor je detektor koji u koristi pasivnu infracrvenu tehnologiju koja omogućuje detekciju isijavanja tjelesne topline.

Kombinirani detektor (PIR/MW) koristi mikrovalnu tehnologiju kako bi preciznije razlučio osobu u pokretu od lažne detekcije isijavanja topline u prostoru.

Postoje i detektori koji se ne aktiviraju na manje objekte (oznaka PET / PET imunnity). Takvi detektori se koriste u prostorima gdje postoji mogućnost lažnog aktiviranja alarma od strane manjih životinja, kućnih ljubimaca, psa čuvara i slično.
Vanjski detektori imaju veću IP zaštitu, tj. otpornost na atmosferske uvijete.

Odabirom fresnel leće detektorima se mijenjaju svojstva namjene. Prema tome razlikujemo širokokutne detektore od uskopojasnih (curtain/zavjesa/zraka).



Slika 19. Fresnelova leća (izvor: http://www.glolab.com/focusdevices/focus.html)

Protuprovalni detektori se razlikuju po načinu povezivanja na centralu pa ih dijelimo na žičane i bežične.

Slika 20. Žičani detektor pokreta „DT2000“ (izvor:https://www.elmospa.com/en/products/active/intrusion-detection/wired-detectors/indoor-wired-detector/dt2000)

Važna svojstva detektora su funkcije:

- tamper - mikro prekidačem ili zrakom detektira mogućnost sabotaže, tj. otvaranja kućišta detektora;
- antimasking - lećom detektira sabotažno prekrivanje detektora ili sprejanje leće;
- gyro - funkcija koja detektira sabotažno zakretanje ili pomicanje detektora
- white-light - funkcija koja onemogućuje sabotažu detekcije zraka bijelim svjetlom
- routing-code ili 2way - funkcija koja konstantno održava komunikaciju detektora i centrale zaštićenom i ne dozvoljava sabotaži prekid ili ometanje komunikacije

5.3.4. Sustav video nadzora

Video-nadzorni sustav služi za protuprepadna djelovanja kojemu je zadaća odvraćanje potencijalnog počinitelja od počinjena kaznenog dijela te njegovo pohranjivanje na određeni medij. Ako i dođe do kaznenog djela, pomoću ovog sustava lako se mogu utvrditi okolnosti i počinitelj.

Danas se najčešće koriste dvije tehnologije video sustava.

- CCTV (eng. ″Closed Circuit Television network″) mrežna zatvorena televizijska petlja
- IP (Internet protokol) sustav video nadzora

Osnovne karakteristike CCTV video sustava:

- fleksibilno povezivanje (LAN, ADSL, Internet, mobilne mreže i sl.)
- prijenos u stvarnom vremenu i kristalno čista slika
- digitalno video snimanje
- inteligentno i automatsko upravljanje
- telemetrijska kontrola (daljinska kontrola)
- skalabilnost (lako se prilagođava potrebama korisnika)
- nadzor preko interneta i mobilnih mreža [24] CCTV sustav se sastoji od:
- sigurnosne kamere (analogna ili digitalna)
- kablovi (RJ45 ili RG59)
- video rekorderi
- nadzorna jedinica (ekran ili mobitel)

Slika 21. CCTV nadzorna kamera (izvor: https://www.cctvcamerapros.com/CCTV-Security-Cameras-s/50.htm)

Mrežni video-nadzorni sustavi omogućavaju korisnicima da gledaju, nadgledaju i snimaju video i audio putem mreža kao što su LAN mreže, širokopojasni Internet, telefonske i mobilne mreže. U odnosu na tradicionalne analogne sustave video nadzora mrežni sustavi prenose video sa udaljenih lokacija od bilo kuda i u bilo koje vrijeme prema korisniku bez obzira na njegovu lokaciju. Korištenjem mrežnih sustava video nadzor postaje prikladan i komforan, nudi platformu za integraciju kao i za razvoj mnogih drugih aplikacija kod kojih je video-slika koja je emitirana uživo također kvalitetna sa udaljenih lokacija i od velikog je značaja

IP (Internet protokol) kamere ili digitalne kamere prenose videozapise bežično preko računalnih mreža. Imaju bolju kvalitetu snimanja i mogućnost povezivanja velikog broja kamera na nadzorni sustav. Koriste PoE (eng. power of ethernet) čime se izbjegavaju kablovi pri instalaciji i imaju dvosmjerni audio izlaz za komunikaciju s ljudima s druge strane kamere. Kada se IP kamera poveže s mrežom, štićeni prostor se može nadzirati s bilo kojeg mjesta. Na računalu je potrebno otvoriti web preglednik unijeti statičku IP adresu ili DDNS(eng. Dynimac Domain Network Server) ime domene kamere i pratiti prijenos uživo.[16]

Slika 22. IP nadzorna kamera (izvor: https://www.elmospa.com/en/products/active/cctv/ip/dome-shooting-systems-2/pro223si1)

[16] https://www.safetrolley.com/how-cctv-works

Kada sigurnosna kamera pošalje video signal, taj signal mora biti negdje dokumentiran. Za to se koriste video snimači. Ako video signal šalje CCTV analogna kamera koristi se digitalni video snimač DVR (eng. Digital Video Recorder), a ako video signal šalje IP digitalna kamera onda se koristi mrežni video snimač NVR (eng. Network Video Recorder).[17]

Slika 23. NVR I DVR snimači (izvor: https://getsafeandsound.com/2018/12/nvr-dvr-channels)

Slika 21. prikazuje poleđinu NVR i DVR snimača. Glavna karakteristika im je koliki broj kanala sadrže. Razlika je u tome što DVR snimač može imat onoliko kamera priključeno koliki mu je broj kanala, dok se kod NVR snimača može spojiti više kamera na jedan kanal, a najčešće je ograničenje dvije kamere na jedan kanal. Digitalni video prijenos se emitira preko lokalne mreže LAN pomoću mrežnog (CAT5 ili CAT6) kabela. Napajanje na kamerama je osigurano preko mrežnog kabela pomoću PoE adaptera ugrađenih u kamere i omogućene preko PoE prekidača (eng. PoE switch). Ethernet kabel za svaku kameru priključen je u prekidač koji se napaja u mrežni usmjerivač (eng. ″router/hub″). Na prekidač su spojeni prijenosno računalo zbog postavki sustava te NVR snimač video signala. Na snimač je spojen monitor preko kojeg se nadzire štićeni objekt, a spojen je HDMI kabelom.

[17] https://www.safetrolley.com/how-cctv-works

6. ZAKLJUČAK

Računalni sustavi predstavljaju vrstu alata bez koje u današnje vrijeme je nezamisliv iole ozbiljniji posao. Zbog povezanosti na globalnoj razini u svim segmentima radnog okruženja pojavljuje se potreba za sve većim količinama podataka, a i samim tim vrsta podataka koje ne bi željeli podijelit sa drugim neovlaštenim osobama. Takvim neovlaštenim osobama računalni sustavi ili dana centri, kako ih još možemo zvati, predstavljaju metu u kojoj oni vide ogromnu količinu podataka koje bi se mogli okoristili u svoju korist, a i u većini slučajeva na našu ogromnu štetu.

Zato se računalni sustavi osim zaštitom u virtualnom okruženju, zaštićuju i zaštitom fizičkog okruženja, ne bi li se smanjila mogućnost nastanka štete krađom podataka neposredno na samim sustavima ili pripremom za neku buduću radnju. Za tu svrhu koristimo tehničku zaštitu kao jedan segment zaštite u cjelini. Iz tog razloga tehnička zaštita mora biti stručno i kvalitetno odrađena da se rizik smanji na čim manju moguću mjeru.

Literatura

Knjige:

1. Lawrence J. Fennelly,(2004), Effective Physical Security, Elsevier Inc.
2. Continuity, S. a. O., (2007), Disaster Recovery. Georgetown University: University Information Services
3. Ribarić, S., (2011) Građa računala, arhitektura i organizacija računarskih sustava
4. Delišimunović, D.,(2002), Suvremeni koncepti i uređaji zaštite, Zagreb, I.T.Graf
5. Delišimunović, D.,(2006), Management zaštite i sigurnosti, Zagreb, Pragmatekh

Internet izvori:

1. https://mydataknox.hr/o-nama/nasi-data-centri#!, učitano 19. kolovoza 2020. godine
2. https://www.setcor.com/o-nama/podatkovni-centri/#!, učitano 19. kolovoza 2020. godine
3. https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-06-304.pdf, učitano 25. kolovoza 2020. godine
4. http://estudent.fpz.hr/Predmeti/I/Informacijski_sustavi_mreznih_operatera/Materijali/07_-_Zastita_informacijskih_sustava.pdf, učitano 23. kolovoza 2020. godine
5. https://realpars.com/fire-alarm-system, učitano 25. kolovoza 2020. godine
6. https://www.elprocus.com/heat-detector-circuit-working/, učitano 28.kolovoza 2020. godine

Popis slika:

SAŽETAK

Cilj ovog rada bio je prikazati sigurnost računalnih sustava kroz segment tehničke zaštite radi razumijevanja funkcioniranja iste, a kao mogućnost za poboljšanje same sigurnosti samih sustava. Kroz ovaj rad osvrnuli smo se na segment sigurnosti i strategiju te uzeli realni primjer iz poslovnog sektora gdje se može primijeniti ta zaštita. U cilj je bila uključena predstavljanje opreme koja se može naći na domaćem tržištu, a u njihovoj kombinaciji čine jednu od ozbiljnijih cjelina za zaštitu štićenih objekata. Provedba je ključna i zahtijeva mnogo financijskog odricanja kroz duži vremenski periodi, kako bi se uspješno sačuvao integritet sustava i ostvario cilj. Svoj doprinos moraju dati svi uključeni u projekt implementacije, od tehničara na montaži opreme do projektanata koji smišljaju sam sustav. Mnoge tvrtke širom svijeta koriste tehničku zaštitu radi ostvarenja sigurnosti svoje imovine i zaposlenika.

KLJUČNE RIJEČI: sigurnost, tehnička zaštita, računalni sustavi, prijetnje, fizička sigurnost, regulative, zakon

SUMMARY

The aim of this paper was to present the security of computer systems through the segments of technical protection of radio understanding of their functioning, as an opportunity to improve the same security of the systems themselves. Through this paper, we looked at the security segment and the strategy took a real example from the business sector where protection can be applied. The aim includes the presentation of equipment that can be found on the domestic market, and in their combination they form one of the more serious units for the protection of protected facilities. Implementation is crucial and requires a lot of financial sacrifice over a period of time, as the integrity of the system is successfully preserved and the goal achieved. Everyone involved in the implementation of the project must contribute, from the technical equipment on the assembly equipment to the designers who think of the system. Many companies around the world use technical protection to ensure the safety of their assets and employees.

KEY WORDS: security, technical protection, computer systems, threats, physical security, regulations, law