BOJANIĆ Nebojša[1]

ELEKTRONSKI SIGURNOSNI SISTEMI TEHNIČKE ZAŠTITE OBJEKATA

ELECTRONICS SECURITY SYSTEMS IN TECHNICAL SECURITY PROTECTION OF OBJECTS

Sažetak

U ovom radu prikazane su osnovne komponente funkcionisanja elektronskih sistema tehničke zaštite, koje se do danas primjenjuju kao zaštita na objektima. Određen je pojam tehničke zaštite, a prikazane su i vrste, te praktične mogućnosti tehničke zaštite. Iz rada se vidi, da se elektronski uređaji koji se koriste u svrhu zaštite objekata, ne mogu efikasno koristiti, ako nisu uvezani u određene funkcionalne sisteme. Značaj bezprijekornog funkcionisanja tehničke zaštite pridaje se ljudskom faktoru, što se ističe u ovome radu, te primjeni kriminalističkih sadržaja u realizaciji zaštite. Naročita pažnja poklonjena je pravilima ponašanja operatera i čuvara, koji manipulišu uređajima tehničke zaštite. Na njima je velika odgovornost, da ne dopuste neovlašteni pristup, kako sistemima zaštite, tako i samim objektima pod zaštitom.

Ključne riječi: *Tehnička zaštita, elektronski sistemi, kriminalistički sadržaji, alarmni sistemi, senzorska zaštita, video nadzor, centralni nadzorni sistem.*

Uvod

Čovjek danas živi u vremenu svakodnevnog rapidnog tehnološko-tehničkog napretka. Takav ubrzan razvoj tehničkih sredstava, omogućio je isto tako brz razvoj proizvodne tehnologije, čime su se znatno poboljšali uslovi života i rada, omogućena je brza, efikasna i jeftina proizvodnja roba široke potrošnje, ubrzani su, prošireni i

[1] Mr. sc., viši asistent na Fakultetu kriminalističkih nauka u Sarajevu

pojednostavljeni putevi cirkulacije tokova novca, a standard stanovništva (naročito u razvijenim zemljama) je u konstantnom porastu. Povećanje standarda stanovništva, polarizacija svijeta na bogate i siromašne, izumiranje srednjeg staleža u zemljama u tranziciji, uticaj američkih akcionih filmova, porast narkomanije, kao i lokalnih idola mladih koji su se preko noći obogatili na nezakonite načine, te želja dijela stanovništva za brzim sticanjem bogatstva i rješavanjem egzistencijalnih problema, jedan su od faktora porasta imovinskog kriminaliteta. Sa porastom kriminaliteta raste i opšta nesigurnost i strah za bezbjednost stanovništva, te bezbjednost različitih privrednih subjekata i njihove imovine. Ipak, isti taj razvoj nauke i tehnike, doprinijeo je razvju različitih tehničkih sredstava i uređaja koji su se počeli masovno primjenjivati u zaštiti ljudi i imovine, ali i kao preventivna mjera u odvraćanju kriminalaca od protivpravnih radnji. Obzirom da je cilj kriminalaca da se zaobiđu sistemi zaštite, na tehničkim naukama i kriminalističkoj nauci je, da iznađu načine i sredstva da se postigne što veći nivo sigurnosti i organizacije zaštite lica i imovine u tehničkom smislu. Tehničke nauke su tu da obezbjede tehnička sredstva zaštite, Zakon i pravilnici o tehničkoj zaštiti su tu da daju pravni okvir i standarde kojih se treba pridržavati u izvedbi tehničke zaštite, a kriminalistička nauka temelj realizacije tehničke zaštite, tj. da tehničkim sredstvima i pravnim okvirima da taktičko-tehničke sadržaje u njihovoj upotrebi.

Da bi tehnička zaštita bila svrsishodna i ispunjavala svoj cilj, potrebno je da se uveže u sisteme i da je izvršni - finalni sistem spojen na centralni dojavni sistem, koji se mora nalaziti na jednoj lokaciji, najčešće u agenciji za obezbjeđenje lica i objekata. U tom smislu, cilj ovog rada je da se prikažu neki oblici elektronske tehničke zaštite, standardi i mogućnosti njene primjene, te da se kroz zaključke ukaže na postupanje ovlaštenih lica koji upravljaju i neposredno operišu elektronskim sistemima tehničke zaštite, te su i odgovorna za sigurno i pouzdano funkcionisanje sistema.

Treba reći da, u sistemu elektronske i sigurnosne tehničke zaštite veliki značaj imaju sistemi protivprepadne zaštite, sistemi javljanja požara i štetnih gasova te video nadzor, upotreba različitih detektora i senzora. Da bi sistem uspješno funkcionisao,

nezaobilazan je faktor čovjek, te je u tom smislu neophodno uspostaviti vezu korisnik – zaštita – sigurnost.

Određenje pojma

Posmatrajući kroz prizmu zakonodavca[2], vidi se da je pojam tehničke zaštite određen veoma široko, te da u zakonskim okvirima omogućava upotrebu najšire palete tehničkih uređaja i sredstava. Tehnička zaštita ljudi i imovine predstavlja takvu vrstu zaštite, koja se provodi različitim tehničkim sredstvima i metodama, čiji je cilj sprečavanjre različitih oblika protivpravnih radnji koje su usmjerene prema štićenim licima i imovini, u skaldu sa važećim pravnim propisima. Riječ je o protivprovalnim i kontradiverzionim mjerama zaštite, kao i kontroli pristupa za sve vrste objekata, uz pomoć elektronskih, kompjuterskih, video i telekomunikacionih sistema. Imovina koja se štiti može biti pokretna i nepokretna. Objekti koji se stavljaju pod tehničku zaštitu najčešće mogu biti: a) različiti proizvodni objekti od opšteg društvenog interesa ili visoke vrijednosti, koji su izloženi velikom rziku od krađe (npr. različiti objekti za izradu nakita); b) ekološki i tehnološki riskantni industriski objekti, koji u pravilu imaju kontinuran tok proizvodnje (npr. fabrike lijekova – Bosnalijek, rafinareija nafte i maziva u S/B Brodu, Modriči, Polihem i sl.); c) industrijski kompleksi (željezare, ciglane, cementare, i sl.); d) objekti od strateškog značaja (termo i hidroelektrane, vodovodi i rezervoari i sl.); e) objekti od posebne vrijednosti (banke, draguljarnice, ambasade i sl.); f) svi drugi objekti čiji vlasnici zahtjevaju zaštitu i žele osjećaj sigurnosti. Kada se radi o primjeni većih sistemaa tehničke zaštite, najčešće je riječ o nepokretnoj imovini. Međutim, različite vrijednosti pokretne imovine, i rizik poslova koji se obavlja sa takvom imovinom, kao što je slučaj sa transportom novca, plemenitih metala i drugih predmeta od vrijednosti, zahtjeva upotrebu sofisticiranih sredstava tehničke zaštite. Posmatrajući područja života i djelovanja ljudi gdje je tehnička zaštita primjenjiva, može se s pravom konstatovati da se

[2] Prema članu 4., stav 3. Zakona o agencijama za zaštitu ljudi (Sl. Novine Federacije BiH, br. 50/2002), tehnička zaštita predstavlja zaštitu ljudi i imovine tehničkim srededstvima i opremom koja je namjenjena za te potrebe.

tehnička zaštita ljudi koristi kao mjera prevencije i to, kako konstatuje i R. Rađenović (Rađenović, R., 2003:100) u slučajevima:

otkrivanja i uklanjanja eksplozivnih, zapaljivih, radioaktivnih i drugih opasnih sredstava (riječ je o kontradiverzionoj zaštiti - KDZ);

otkrivanja i uklanjanja protivprislušnih sredstava (protivprislušna zaštita);

utvrđivanja i otklanjanja tehničkih neispravnosti na uređajima i instalacijama u objektu pod zaštitom;

sprečavanja tajnog ili nasilnog prodiranja u objekat, određene prostorije, sefove i slične objekte pod zaštitom (zaštita od tajnog ili nasilnog ulaska u štićeni objekat);

zaštita od požara (protivpožarna zaštita);

sprečavanje, odnosno onemogućavanje ugrožavanja bezbjednosti objekta pod zaštitom upotrebom savremenih borbenih sredstava;

Suštinski cilj postavljanja tehničke zaštite je, kao i što navodi M. Jamaković (Jamaković, M., 2000:59) zamjena čovjeka u trenucima kad gubi budnost zbog biološke potrebe za snom ili iz određenih razloga zbog kojih u momentu napada na objekat odsustvuje sa radnog mjesta. Ovome se može dodati i to, da je cilj primjene tehničke zaštite postaviti što savršeniji sistem za detekciju napada i primjena preventivnih mjera u cilju odvraćanja od napada. Iz svrhe korištenja tehničke zaštite proizilaze i same vrste tehničke zaštite koje se koriste u objektima i prostorima pod zaštitom. Shodno Pravilniku o tehničkim napravama, sredstvima i opremi koja se može koristiti za obaljvanje poslova tehničke zaštite, može se reći da postoje dva osnovna vida tehničke zaštite[3].

[3] Član 3. Pravilnika o tehničkim napravama, sredstvima i opremi koja se može koristiti za obaljvanje poslova tehničke zaštite, Službene novine Federacije BiH, br. 54/2002. U daljnjem teksu samo pravilnik.

sistemi za sprečavanje nedopuštenog pristupa objektima pod zaštitom, i
elektronski i sigurnosni sistemi zaštite objekata.

Kada je riječ sistemima za sprečavanje nedopuštenog pristupa objektima pod zaštitom, treba reći da se tu primarno radi o mehaničkim tehničkim sredstvima, kao što su specijalne ograde, rampe, barikade, protivprovalna vrata i drugi mehanički sistemi, kojima neposredno rukuje (manipuliše) čovjek. Zatim, u ovu grupu spadaju i sve vrste brava sa serijskim brojevima ili kodovima, specijalne građevniske konstrukcije, kao i oprema za skladištenje i čuvanje predmeta i dokumenata (kase, trezori, ormari i sl.).
Elektronski sigurnosni sistemi zaštite sastoje se od vlastitih komponenata, koje treba da omoguće:

stalni nadzor nad objektom pod zaštitom sa jednog mjesta – to podrazumijeva da na jednom mjestu mora biti uspostavljen centralni nadzorni sistem, sa kojeg se kontroliše i manipuliše cjelokupnim sistemom tehničke zaštite;

otkrivanje i evidentiranje nedopuštenog stanja – neophodno je registrovati bilo koji neovlašteni ili nasilni ulazak, odnosno pokušaj ulaska u objekat pod zaštitom ili samo neki njegov dio, kontrolu i nadzor radnika i službi unutar samog objekta pod zaštitom, pokušaj onesposobljenja sistema zaštite i sl.;

provedbu plana postupanja u vanrednim situacijama – takvim planom treba biti predviđeno da se automatski provedu dodatne aktivnosti u slučaju povrede prostora. Takvim mjerama trebalo bi, primjera radi, mehanički blokirati određene prolaze, prekinuti napajanje električnom energijom, izvršiti automatsko javljanje drugim ovlaštenim licima i MUP-ovima, drugim javnim komunalnim službama i sl.;

rekonstrukciju događaja, odnosno okolnosti koje su prethodile nastupanju vanrednog stanja;

nadzor nad radom i budnosti čuvara zaduženih za sigurnost i provođenje propisanog radnog režima na objektu;

Treba istaći, da sve aktivnosti u vezi, kako sa mehaničkom, tako i elektornskom zaštitom, mora da obavlja ovlašteno službeno lice, agencije za zaštitu lica i objekata ili orgnana unutrašnjih poslova.

Kao što lice koje rukovodi i upravlja zaštitom treba imati ovlaštenje nadležnog organa unutrašnjih poslova, tako i sistemi tehničke zaštite trebaju imati određeni certifikat koji im garantuje standardizaciju, pouzdanost i sigurnost u radu. Svaki proizvođač uređaja, koji se koriste u svrhe tehničke zaštite ne smije plasirati na tržište uređaje i opremu koji ne zadovaljavaju najviše svjetske standarde. Riječ je standardima ISO 9001, 9002 i sl.

Vrste i praktične mogućnosti nekih oblika elektronske tehničke zaštite

U realizaciji sprovođenja elektronske i sigurnosne zaštite objekata, treba poći od značaja, vrste i veličine objekta koji je predmet zaštite. Isto tako, ne treba zaboraviti ni finansijski momenat investitora. No, treba istaći da, ukoliko investiror raspolaže sa većim finansijskim sredstvima, i modernijom tehnologijom u izvedbi sistema tehničke zaštite, u toliko je veći procenat sigurnosti zaštite objekta. Ipak, može se konstatovati i da su same mašine ili uređaji bespomoćni bez faktora čovjeka, koji svjesno prema zakonskim propisima, ali i pravilima, standardima i načelima određene struke upravlja sa njima. Prema tome, nemože se sa sigurnošću utvrditi da ima 100% uspješnih sistema tehničke zaštite. Kako se tehnika razvija i sistemi zaštite usavršavaju, tako se i kriminalci obučavaju, tj. školuju i usavršavaju da zaobiđu i najsavremenije metode elektronske tehničke zaštite.

Elektronska tehnička zaštita može se podijeliti u sljedeće grupe:
alarmni sistemi;

sistemi senzorskih detektora koji kontrolišu određena stanja u objektima na bazi ultrazvučnih, invracrvenih, ultraljubičastih talasa, detekotra vibracija i potresa, radio detektora, geoloških detektora, lasera i sl.;

video nadzorni sistemi uz pomoć sve jeftinijih i specijalizovanih elektronskih kamera, termovizijskih uređaja i ostale prateće video opreme;
uređaji za kontrolu i zaštitu pristupa objektu provjerom individualnih identifikacionih podataka na elektronskom principu (barcode);

elektronski sistemi visokog stepena složenosti bazirani na kompjuterskoj tehnologiji za upravljanje radom svih podsistema zaštite i njihovu međusobnu koordinaciju, razmjenu informacija i vezu sa spoljnim svijetom i pratećim izvršnim podsistemima.

Alarmni sistemi

Osnovna namjena bilo kojeg alarmnog sistema je detekcija pokušaja napada na objekat pod zaštitom, prevencija i odvraćanje od napada. Alarmni sistemi nemaju tu moć da uhvate napadača, ali zato do izražaja dolazi faktor čovjek, koji će pravovremeno reagovati na znak alarma, te preduzeti mjere da se napadač otkrije i liši slobode. Alarmni uređaji funkcionišu pomoću alarmnih centrala na koje se uvezuju alarmni detektori, alarmne sirene, digitalne tastature ili ključevi za jednostavno upravljanje sistemom, telefonski ili bežični automati, za prenos alarma na daljinu. Dobar sistem tehničke zaštite pretpostavlja uvezivanje više sistema, kao što su alarmni uređaji, senzori, i video nadzor. Međutim, kako se povećavaju zahtjevi za višim stepenom sigurnosti, tako se povećava složenost sistema i cijena samog sistema zaštite.

Osnovni principi funkcionisanja alarmnog sistema zaštite su:

Potpunost – zaštita imovine i ljudi kao osnovna namjena uspostave sistema zaštite pretpostavlja pravilnu procjenu bezbjednosne situacije na i oko objekta i analizu svih mogućih načina ugrožavanja objekta. Na osnovu navedenog primjenjuju se odgovarajuće mjere, radnje postupci i tehnika.

Odvraćanje – table sa pismenim upozorenjima javno istaknute sa vanjske strane objekta da je objekat pod određenim vidom elektronske zaštite, u ovom slučaju alarmnog sistema.

Visoka pouzdanost sistema – obezbjeđuje se kvalitetnim izborom opreme i kombinacijom više sistema zaštite, te kvalitetnom projektnom dokumentacijom i pravilnom montažom. Za pouzdanost sistema potrebno je obezbjediti alarmne centrale odgovarajućeg kapaciteta, alternativne izvore napajanja električnom energijom, jedan ili više detektora - senzora (zavisno od potrebe) istog ili različitog tipa, sirene ili svjetlosnu signalizaciju. Kao dodatna oprema, koja povećava stepen uspješnosti na alarmne sisteme može se montirati telefonski javljač, bežični panik tasteri i dimni detektori. Izbor alarmne centrale vrši se u skladu sa zahtjevima korisnika i namjenom objekta. Na centrale je moguće postaviti veći broj šifratora, tako da je u manipulaciji sistema potrebno obratiti pažnju na bezbjednost šifri. Prednost modernih alarmnih centrala je mogućnost njihove parcijalne podjele na više dijelova, u zavisnosti od oblika i vrste objekta, kojima bi se trebalo pristupiti sa više različitih korisničkih lozinki i jednom glavnom lozinkom.

Senzorska zaštita

Riječ je o sistemu zaštite koja podrazumijeva primjenu velikog broja različitih detektora (senzora) koji kontrolišu određena stanja u, na i oko objeka pod zaštitom. Riječ je o stanjima otvorenosti ili zatovrenosti prozora, registrovanju kretanja u zoni pod zaštitom, nasilnom otvaranju vrata, pojavi dima, svjetlosti i sl na bazi primjene: geofona (detektor vibracije – pogodni za ograde i zemlju), IC i dualni[4] senzori (registruju promjene toplote i temperature), i mikrotalasnih senzora (registruju i porede prvobitno stanje u prostoru koje pokrivaju u odnosu na prethodno stanje), fotoćelija (registruju presjecanje svjetlosnih zraka), hemijskih (detekcija otrovnih, eksplozivnih i zapaljivih gasova i para) senzora i sl. Uspjeh ovog tipa elektronske zaštite pretpostavlja povezivanje sistema u cjelinu putem posebnih kablova, te sprečavanje lažnog ili fingiranog aktiviranja senzora.

[4] Dualni senzori su pouzdaniji, s obzirom na svoju dualnu detekciju, primjenjuju se u prostorijama sa aspektom temperature, promaje, u prostorijama gdje postoje TA peći, kamini, radijatori, obične peći i sl.

Ovi senzori predstavljaju dodatak sigurnosnim alarmnim uređajima.

Prema namjeni, senzori se mogu podijeliti na senzore za zaštitu periferije[5], za zaštitu prostora, za zaštitu od napada i za zaštitu predmeta.

Postoje i takvi sigurnosni senzori, koji, kada svojim senzorima registruju prisustvo u prostoriji pod zaštitom, aktiviraju određene nervne gasove, što je sa stanovišta pravnih propisa i ljudskih prava često sporno. Isto tako postoje sistemi koji, kada se aktiviraju puštaju zvuk koji je neosjetljiv za ljudsko uho (visoki decibeli), no kod čovjeka izaziva jaku glavobolju ili stanje nelagodnosti, iznemoglosti, mučnine i visokog psihičkog pritiska, te lice želi istog momenta da napusti prostoriju. Riječ je o sistemima koji se zloupotrebljavaju sa aspekta ljudskih prava, i koji su štetni kako za fiziološko, tako i mentalno zdravlje čovjeka, te se nikako ne bi smjeli upotrebljavati. Može se reći da je riječ o jednom obliku obmane, a obmana se (pa osim u određenoj maloj dozi) ne bi smjela upotrebljavati u takvim situacijama, koje mogu rezultirati krivičnim progonom.

I na kraju, treba spomenuti i analizator stresa glasa. Riječ je o jednostavnom uređaju koji radi mjereći mikrotremore u glasu. Kada ljudi lažu dovode se pod stres koji uzrokuje reakciju autonomnog nervnog sistema. Pod stresom se tijelo uzbuđuje, što rezultira pojačanom cirkulacijom krvi iz pravca ekstremiteta, te se tom prilikom naprežu mišići. S obzirom da su glasne žice u principu mišićno tkivo, one se također stežu uzrokujući određene promjene u glasu. Ove male promjene frekventne modulacije u svkakom glasu nazivaju se mikrotremori. Analiza ne zahtjeva bilo kakve kablove i priključke spojene na tijelo. Audio ili video traka koja snima ljudski glas može se analizirati dan ili mjesec nakon što je napravljena. Intervjui, govori ili konverzacije mogu se snimati na traku i analizirati čak i nekoliko godina kasnije. Uređaj je nezavisan od uticaja godina lica koje prolazi analizu, njegovog medicinskog stanja, korištenja droge, te se može koristiti za analizu audio-video traka za vjerodostojnu identifikaciju. Također, ispitanik ne mora

[5] Pod periferijom bi se trebale podrazumjevati granične površine objekta – prozori, vrata, ograde i sl.

prolaziti klasični postupak ispitivanja kao kod poligrafa. U zaštiti objekata značajno je, da se ovaj uređaj može koristiti pri analizi snimljenih telefnoskih razgovora, u kojima se javila indicija da je riječ o nekom napadaču, ili razgovora u prostorijama pod zaštitom gdje se takvi razgovori snimaju. Ovaj uređaj je primarno interesantan kao uređaj za identifikaciju.

Video nadzor i TV sistem zatvorenog kruga (CCTV)[6]

Video nadzor predstavlja posmatranje prostora unutar ili izvan objekta pod zaštitom, prilaznih puteva i ulaza, te kritičnih tačaka na objektu pod zaštitom, i na koncu određenih prostorija u štićenom objektu, koji se realizuje pomoću kamere i posmatrača preko različitih vrsta prenosnih medija, koji mogu biti koaksijalni kabl, telefonska parica ili optički kabl. Posmatranje događaja iz ili pored nekog objekta pod zaštitom na većoj udaljenosti, moguće je pomoću radio uređaja, internet mreže, kao i telefonskih i optičkih kablova.

Digitalni video nadzor, predstavlja savremenu primjenu video tehnike u poslovima tehničke zaštite. U takav sistem ugrađen je, osim kamere i kompjuter, te internet veza od kamere do centralnog nadzornog mjesta. Mogućnosti ovakve vrste video nadzora su u tome, da se slika može isparcelisati i svi podaci i slike se mogu pohraniti na hard disk u kompjuter. Dakle, ovaj sistem je u prednosti u odnosu na klasični video nadzorni sistem, jer omogućuje lak prenos podataka na daljinu putem interneta, i bilježenje na magnetne medije, što zamjenjuje kilometre video trake.

Kao i kod alarmnih sistema, postoje određeni posebni principi ili načela za funkcionisanje video nadzora. Ti principi su:

Osmatranje – omogućava sagledavanje i kontrolu stanja na najznačajnijim punktovima prostorima, kao i procjenu događaja na njima, što olakšava rad službe obezbjeđenja.

[6] CCTV – Closed Circuit TeleVision = TV sistem zatvorenog kruga

Snimanje – omogućava arhiviranje i reprodukciju incidentnih situacija i događaja, kako bi se mogle izvršiti neophodne analize.

Odvraćanje – riječ je o psihološkom dejstvu na lice, koje namjerava da neovlašteno pristupi u zonu pod nadzorom, ili da se agresivno ponaša, saznanjem da će biti uočeno i snimljeno i da će samim tim postojati materijalni dokaz.

Direktan prenos slike sa zone pod zaštitom na monitor – jedna kamera povezana na jedan monitor, a može biti i više kamera povezanih na jedan monitor, što omogućava veći pregled.

Ne treba zaboraviti i princip da se aktiviranje kamere, odnosno reprodukcija slike na monitoru pojavi kao reakcija odgovarajućeg alarmnog senzora. Ovaj način obično se koristi u slučaju potrebe da se obrati pažnja na određene prostore ili da se izvrši arhiviranje kritičnih momenata.

Integracija sa sistemom za kontrolu pristupa – vezano za prethodno, kamere su povezane u jedan cjelokupan sistem i aktiviraju se prilikom neovlaštenog pristupa u zaštićeni prostor.

Uređaji za kontrolu i zaštitu pristupa objektu provjerom individualnih
identifikacionih podataka na elektronskom principu

Kada se govori o uređajima za kontrolu i zaštitu pristupa provjerom individualnih identifikacionih podataka, treba reći, da je riječ o kombinaciji fizičke i tehničke zaštite. Evidentiranje vremena prisutnosti je najniži nivo zaštite koji se sprovodi samo na ulazima i izlazima iz objekata. Svaki zaposleni mora posjedovati određenu identifikacionu karticu, čiji princip rada može da se zasniva prema zahtjevima korisnika na: tehnologiji radio signala (proximity), magnetnog koda, barcode, elektronskog koda (button) sa ili bez fotografije. Za ovaj sistem senzori se postavljaju na ulazna i izlazna mjesta, a njihov broj je u direktnoj zavisnosti od broja zaposlenih i njihovoj koncentraciji na mjestima gdje su učestale radne aktivnosti, i gdje lica treba da se sa sigurnošću identifikuju, kao i u prostorijama gdje su pohranjeni najrazličitiji povjerljivi podaci. Senzori pomoću prikladnog software-a i priključka na kompjuter

odašilju informaciju na centralni server, koji automatski formira datoteku o vremenima i mjestima ulaza i izlaza registrovanih lica: zaposlenih ili posjetilaca u objektima.

Pristup u zaštićene zone predstavlja sljedeći nivo zaštite unutar jedne ili više grupa prostorija u objektu pod zaštitom. Ovaj vid zaštite sprovodi se na osnovu specifikacije spiskova lica, koji imaju pristup u zaštićene zone. Senzori za očitavanje podataka na karticama postavljaju se na razne načine u kombinaciji sa drugim senzorima, kao npr. IC ili dualnim senzorima, koji detektuju prolazak lica. Ovakav vid zaštite moguće je postaviti na sve ulaze i izlaze unutar i izvan objekta.

Elektornski sistemi za dojavu požara

Sistemi za dojavu požara izgrađeni su na principi senzorske reakcije na dim, vatru i toplotu. Njihova je funkcija da otkriju požar u njegovoj ranoj fazi i da spriječe veću imovinsku štetu, slanjem eletronskog impulsnog signala do centralnog nadzornog mjesta, prema kojem je usmjeren sistem. To mogu biti vatrogasne jednice, agencije za zaštitu lica i objekata i sl. Principi rada sistema za dojavu požara su: detekcija požara, upravljanje i kontrola sistemom koju obavlja centrala za dojavu požara, signalizacija koju obavljaju razne sirene i indikatori, komunikacija posredstvom različitih oblika dojavljivača, automatizacija za upravljanje gašenjem, vratima, rasvjetom i evakuacijom. Kriterije kojima se treba voditi pri postavljanju sistema za dojavu požara veoma konstruktivno navodi D. Kauzlarić, koji prema njoj predstavljaju ugroženost prostora, topografska konfiguracija prostora, moguće izvore lažnih alarma, te vrijednosti koje se u prostoru nalaze (Kauzlarić, D., 2003: 63).

Što se tiče samih detektora, koji su i bit problema, oni se razvijaju paralelno sa napretkom i razvojem različitih tehnologija. U odnosu na razvojne tehnologije, ti detektori se mogu podijeliti na analogno adresibilne i konvencionalne. Prednost analogno adresibilnih detektora u odnosu na konvencionalne, može se očitovati u bržoj lokalizaciji detektora, gdje se odmah registruje tačan lokalitet gdje je došlo do pojave vatre; detaljan opis lokacije, što je značajno za

velike objekte; precizno postavljena zona za evakuaciju; podešavanje osjetljivosti i pametni algoritmi; automatska kompenzacija smetnji.

Primjera radi, treba znati i to, da se za zaštitu od požara u razvijenim zemljama izdvaja 1% od nacionalnog GDP-a, jer je izračunato da prevencija smanjuje štete od požara od 2 pa čak do 20 puta.

Kriminalistički sadržaji elektronske zaštite objekata

Prilikom projektovanja i izvedbe sistema, bitno je predvidjeti njegovo autonomno funkcionisanje, kao i vidove zaštite od lažnih alarma i neovlaštenih upada u sistem. Potrebno je napraviti razliku između neovlaštenog i nasilnog upada u sistem ili štićeni objekat. Neovlašteni upad u sistem podrazumjeva sve aktivnosti koje se primjenjuju kako bi se došlo do načina, sredstva ili metoda ulaska u sistem na protivpravan način. Pri neovlaštenom upadu u elektronski sistem zaštite objekata počinilac neizostavno vodi računa, da ne ostavi tragove upada, ili da uništi i najmanji pokazatelj koji će potvrditi upad u objekat ili sistem, ili da će postojati svijest o upadu u sistem nakon protoka određenog vremena. To jednostavno znači, da će se na samo napadaču svojstven način zaobići sistem zaštite kako bi se ostvario njegov cilj. Nasilni upad u sistem zaštite ili objekat pod zaštitom, predstavlja korištenje svih pomoćnih pribora i alata, pomoću kojih će se izazavati vidljiva destrukcija sistema i objekata. Ovakav postupak će proizvesti veliki broj tragova na samom objektu ili sistemu. U daljem radu na izradi projekta, neophodno je odrediti tačnu mikrolokaciju objekata, te izvršiti njegovu orijentaciju u odnosu na druge objekte u njegovoj blizini, kao i na prilazne i odlazne puteve, vremenske prilike, kriminogene i socijalne prilike kraja. Na navedeno se nadovezuje, da je neophodno izraditi procjenu o vrstama opasnosti kojima je izložen objekat predviđen za ugradnju sistema tehničke zaštite, ili kojima će biti izložen u doglednom vremenskom periodu, kao i pravilnu procjenu sopstvenih resursa i raspoloživih sredstava koja će diktirati uvođenje određenog sistema elektronske tehničke zaštite. Treba istaći da ne postoji

univerzalni momenat za uspostavljanje određenog sistema tehničke zaštite objekata.

Autonomnost sistema podrazumjeva njegovu sposobnost da funkcioniše unutar globalnog elektroenergetskog sistema na koji je priključen štićeni objekat i centrala, te da se u slučaju nestanka električne energije, u periodu od nekoliko milisekundi, može preći na alternativne izvore napajanja. Ti alternativni izvori napajanja električnom energijom, mogu biti višeznačni. Riječ je, o agregatima koji se odmah pale nakon nestanka električne energije, o prelasku na drugi trafosistem elektroenergetskog napajanja na kojem nije došlo do nestanka električne energije, te o akumulatorima. Kada sa spominju akumulatori i agregati periodično je neophodna njihova provjera i kontrola ispravnosti. Sistem napajanja preko akumulatora trebao bi da bude takav, da omogući konstantno punjenje akumulatora i njihov puni kapacitet.

Fingiranje alarma predstavlja jedan od najčešćih mogućih načina da se izvrši upad u sistem, čestim lažnim aktiviranjem kako bi se provjeravala budnost čuvara i spremnost da odreaguju na svaki lažni alarm. U tom slučaju, odmah poslije drugog lažnog alarma treba obavijestiti tim za intervencije kako bi se utvrdio uzrok lažnog alarma, odnosno da li postoji neka greška u sistemu. S obzirom da je sistem atestiran, i da su ga projektovali i postavili certifikovani stručnjaci iz agencija za zaštitu ljudi i imovine, svaka utvrđena neispravnost na sistemu prouzrokovaće i materijalnu štetu po agenciju. Sam sistem treba, osim objekta da štiti i samog sebe, npr, da odmah reaguje na presjecanje napojnih vodova ili vodiča od centale do detektora, senzora ili kamera, da samim tim daje određeni alarm.

Najčešća greška koja se javlja pri projektovanju sistema elektronske tehničke zaštite, je ta, da se projektom rijetko planira registrovanje isključenja sistema, te time praktično kompletna zaštita objekta svodi se na ljudski faktor, što se u mnogim slučajevima može odraziti pogrešno, te omogućiti lak pristup napadača objektu.

Prema postojećem Pravilniku[7] ovakvi zahtjevi za izbjegavanjem greške obavezno se imaju primijeniti.

Zaključak

Na kraju, kao zaključak, trebalo bi navesti neka pravila kojih bi se trebao pridržavati ovlašteni službenik agencije za zaštitu lica i objekata, ili drugi službenik, koji radi kao operater u centru za upravljenje elektronskim sistemima tehničke zaštite. Zašto je ovo potrebno navesti? Naime, već je rečeno da, tehnička sredstva, uređaji i druga oprema predstavljaju samo gomilu metala, elektronskih komponenti, stakla i plastike ukoliko nisu u upotrebi. Za njihovu upotrebu zadužen je čovjek. Dakle, faktor čovjek je taj, koji manipuliše i upravlja sistemima tehničke zaštite i prilagođava ih svojim, i potrebama objekta kojeg štiti. Isto tako, namjerno utvrđeno otkazivanje sistema ili njegova sabotaža, odnosno onesposobljavanje, primarno uzrokuje faktor čovjek. Stoga, kao i u šahu, ko ima više stručnog znanja, živaca, koncentracije, budnosti i mudrosti, izlazi kao pobjednik u upravljanju sistemom elektronske tehničke zaštite. Naročito su na upade u sisteme osjetljivi oni sistemi, koji funkcionišu na daljinu posredstvom različitih medija. Treba imati na umu da, viskosofisticiranim elektronskim sistemima zaštite, čiji su temelj funkcioniranja mikroelektronički i informatički uređaji, komponente i podsistemi, mogu pristupiti samo najstručnija lica iz oblasti mikroelektronike i kompjuterske tehnike u cjelini, kao što su visoko inteligentni hakeri, potpomognuti logističkom podrškom drugih lica, kojima je u interesu savladavanje postojećeg sistema zaštite. U tom smislu, za slučaj provale u elektronski sistem zaštite, potrebno je postaviti kriminalističku diferencijalnu dijagnozu, o mogućem počiniocu. Od značaja je i način upada, odnosno savladavanja sistema zaštite. U istrazi je potrebno prvo otkriti uzrok koji je savladao sistem. Način primjene određene tehnologije za onesposobljavanje i savladavanje elektronskih sistema tehničke zaštite objekata, predstavlja na određen način otisak prsta počinioca.

[7] Član 9., stav 3. tačka 1. Pravilnika o tehničkim napravama, sredstvima i opremi koja se može koristiti za obaljvanje poslova tehničke zaštite, Službene novine Federacije BiH, br. 54/2002.

Potrebno je da rukovodilac ili nadzornik – operater tehničkom zaštitom obrati pažnju na moguće simulacije, odnosno fingiranje. Takvo lice mora bit u mogućnosti da dobro procijeni situaciju, da pravovremeno pozove pomoć, i u svemu da uvijek bude budan i spreman za vanredne situacije. Operater mora shvatiti i naučiti kako da razlikuje pravi napad od fingiranog napada. U svrhu obuke, potrebo je podučiti sve zaposlene da svaki, pa i najmanji incident prijavljuju i registruju, te da ne prave razliku između sitnog, na izgled beznačajnog i krupnog incidenta. Isto tako, agencija koja je nadležna za obezbjeđenje objekata treba da ima tačno utvrđen plan mjera i aktivnosti za rekaciju na incidente. Jedna od mogućnosti prevencije lažnih alarma je pravilno rukovanje, manipulacija i redovno održavanje sistema.

Potrebno je da se u video nadzoru aktivno prati situacija na objektu koji pokriva kamera, da se prate kretnje i aktivnosti ljudi. U sprezi sa fizičkim obezbjeđenjem, posjetioci u objektima pod zaštitom, koji imaju ograničen pristup ljudi iz vana, pored zaduženja sa gostujućim elektronskim magnetnim karticama ili bar kodovoima, trebaju ostaviti svoje identifikacione podatke na ulazu, našta upozorava i K. Mitnik (Mitnik, K., 2003:328). Također, ovlašteno lice na ulazu u objekat trebalo bi da fotokopira identifikacioni dokument stranke, a sve to da se prati i videonadzorom. Isto tako, ulazak u objekat pod zaštitom može biti na vrlo jednostavan način: da napadač ugovori posjetu sa nekim zaposlenim, što mu omogućava da slobodno hoda po objektu, u krugu i unutar objekta. U tom slučaju, na operateru video nadzora je velika odgovornost, jer mora da prati sve registrovane posjetioce i zaposlene, te njihove međusobne kontakte, te da registruje sve sumnjive situacije. Kada se govori sumnjivim situacijama, postavlja se pitanje, koji to znaci mogu upozoriti na mogući incident ili napad na objekat? Takve situacije mogu biti: predstavljanje kao odgovorno lice i naglašavanje razloga hitnosti kako bi se neometano ušlo u objekat ili sistem zaštite, bez identifikacionih markera (najčešće bi se napadač mogao koristiti lažima, da je usljed žurbe vezane za slučaj koji je hitan, zaboravio identifikacione oznake, ili se poziva na odgovrna lica iz sistema zaštite ili samog objekta koji se štiti. Kao još jedna indicija može se pojaviti odbijanje prihvatanja identifikacionog koda na magnetnim karticama ili šifre na elektronskim bravama, koje su pod nadzorom, a koje se uzastopno

ponovalja. Može biti indicija konstantni pokušaji neovlaštenog ulaska u objakat ili sistem. Dijeljenje komplimenata zaposlenicima od strane posjetilaca, kao i određeno šarmiranje službenika može biti također, indicija pokušaja napada na objekat, ili pokušaja da se dođe do povjerljivih informacija od značaja za funkcionisanje tehničkog sistema zaštite.

Naročito je potrebno da operater ovlada tehnikama obmane, kako bi iste mogao veoma lako uočiti ili prepoznati. Upravo najveći i najsposobniji obmanjivači su stručnjaci iz oblasti elektornike i informatike, te raspolažu sa dobrim, kako stručnim, .tako i verbalnim obmanjivačkim sposobnostima. U tom smislu, operater na elektronskim uređajima tehničke zaštite treba da pazi kada putem interneta ili elektronske pošte dobija besplatne, naizgled korisne software, koje bi mogao da instalira. Upravo na njima bi se mogla kriti "buba" koja će automatski odaslati sve podatke ključne za sistem zaštite, kako bi se moglo neovlašteno pristupiti. Također, pažnju treba usmjeriti na slanje virusa ili tzv. "trojanskih konja" preko e-mail poruka, kao i upotreba lažnih dijaloških okvira u ponovnom "logiranju" za rad na sistemu. Moguće je da napadač na takav način instalira programe koji će snimiti načine i redoslijed operaterovih pritisaka na tastaturu prilikom upotrebe sistemskih programa. Jedna od velikih opasnosti krije se u direktnom kontaktu sa napadačem na radnom mjestu. Stoga bi operater trebao biti oprezan i nikada na svoje deskove i radne pultove ne bi trebao/smio ostavljati pristupačnim diskete, CD-ove i druge magnetne medije, koji služe za pohranjivanje podataka. Također ni lozinka ne smije biti nigdje zapisana, osim da ostane kao engram, zapisan u mozgu.

Isto tako, operater treba da je upoznat sa načinima saradnje sa policijom. U tom slučaju neophodno bi bilo da postoji uvijek slobodna telefosnka linija za slučaj potrebe poziva timu za intervencije ili policiji, vatrogascima ili hitnoj pomoći. U slučaju potrebe, potrebno je da pravi svoje interne zabilješke, koje će upotrijebiti prilikom davanja informacija policiji, ili na sudu, ako bude pozvan kao svjedok.

Operateri, kao i nadležna odgovorna lica, ne bi trebali saopštavati preko telefona ili bilo kojeg drugog medija koji prenosi informacije

bežičnim ili žičnim putem, osjetljive informacije ili razmjenjivati podatke koji su direktno vezani za funkcionisanje sistema. Potencijalni napadači mogu prisluškivati razgovore kako na licu mjesta, tako i pomoću prislušnih uređaja. Različitim skenerima mogu doći do frekvencije na kojoj radi mobilni ili bežični telefon, te im onda nije problem slušati razgovore i upijati informacije. Opasnost se krije i prilikom korištenja govorne pošte (tzv. "voice mail"), gdje može biti snimljen glas operatera, ta kao takav biti iskorištena za upad u sistem.
Najmanje dva puta godišnje potreban je remont, odnosno servis, a generalna provjera rada elektronskog sistema tehničke zaštite potrebna je i više puta (čak šta više i jednom mejsečno).
Prema tome, tek kada se steknu dovoljne spoznaje o mogućnostima i potrebama zaštite, biće moguće i analizirati problem, odabrati kriterije kojima će se upravljati prilikom odabira o mjerama zaštite, koje će se primijeniti, uspostaviti kontolne mehanizme za provjeru primijenjenih mjera, te izvršiti periodično analiziranje svih aktivnosti i mjera koje su korištine u sistemu zaštite.

I na kraju, treba reći da funkcionisanje elektronskog sistema tehničke zaštite, kao i sistema zaštite objekata uopšte, zavisi i od bezbjednosne kulture ljudskih potencijala unutar samog objekta, bez obzira na njegovu idealnu postavku. U ponašanje ljudskih resursa unutar objekta (najčešće zaposlenih ili držaoca objekta) treba ugraditi i poštivanje normi i standarda koji će povećati nivo bezbjednosti objekata sa aspekta faktora čovjeka.

Abstract

This paper presentes the basic components in function of electronic systems of technical protection which is used for security protection of objects today. At first, it is defined the term of technical security protection, also as types and practical possibilities of it. In this paper, you can see that electronic equipment used in protection of objects, is not able to use efficently, unless it is connected in special functional systems. The significance of perfect function of technical security protection, is credibility of human resource, so it is emphasized in this paper, also as application of crime contents in protection realisation. The particular focus is upon proper conduct of guards and operatores, who manipulate

with techinical security protection equipment. They bear enormous responsibility, to forbid unauthorized access, nor protection systems nor objects under protection.

***Key words**: techinical security protection, electronic system, crime content, alarm systems, sensors systems, video surveillance, central surveillance system.*

OSNOVNA I KONSULTOVANA LITERATURA

1. Basarić, M. i Vejzagić, N. (1998): "Kriminalistika II (tehnika)", Sarajevo, FKN
2. Jamaković, M. (2000): "Policijska tehnika (skripta), Sarajevo, FKN
3. Mitnik, K. (2003): "Umjetnost obmane", Beograd, Mikro knjiga
4. Pravilnik o tehničkim napravama, sredstvima i opremi koja se može koristiti za obaljvanje poslova tehničke zaštite, Službene novine Federacije BiH, br. 54/2002
5. Rađenović, R. (2003): "Bezbjednost ličnosti i objekata", Beograd
6. Vejzagić, N. (2003): "Tehnička zaštita", Sarajevo, Priručnik za obuku kandidata koji će obavljati poslove fizičke i tehničke zaštite u agencijama za zaštitu ljudi i imovine"
7. Modly, D. (2003): "O čemu trebaju voditi računa zaštitari u svom svakodnevnom radu", bilješke
8. Modly, D. i Korajlić, N. (2002): "Kriminalistički rječnik", Centar za kulturu i obrazovanje, Tešanj
9. Kauzlarić, D. (2003): "Sustavi za dojavu požara", Zagreb, Svijet osiguranja, br. 2.
10. Flood, P.: http://campus.umr.edu/police/cvsa/patflood.htm (03. 02. 2003)
11. Zakon o agencijama za zaštitu ljudi i imovine, Službene novine Federacije BiH, br. 50/2002.