Dr Milojko Jevtović,
profesor, dipl. inž.

ELEKTRONSKI SISTEM ZA INTEGRISANU TEHNIČKU ZAŠTITU VOJNIH OBJEKATA

U radu se analizira koncepcija integrisane zaštite vojnih objekata i prostora korišćenjem elektronskih sistema zasnovanih na primeni računara i programskog upravljanja. Opisana je struktura sistema i njegove funkcije. Dat je pregled elemenata jednog našeg sistema za integrisanu zaštitu, kao što su: računar, senzorski terminal, kartični terminal, različiti tipovi senzora, i navedene njihove bitne tehničke karakteristike. Takođe su analizirana neka pitanja primene elektronskih sistema (projektovanje, nivo zaštite, ekonomičnost, uloga fizičkog obezbeđenja). Naglašen je značaj elektronskih sistema u zaštiti vojnih objekata, kao i mogućnosti njihovog razvoja i domaće proizvodnje.

Uvod

Korišćenje elektronskih sistema za integrisanu tehničku zaštitu vojnih objekata kod nas se, ponegde, postavlja kao dilema. U inostranim armijama takva dilema ne postoji. Elektronskim sistemima pridaje se izuzetna važnost u zaštiti vojnih objekata, a od njih se zahteva da zadovolje dva osnovna zahteva i to:

- da obezbede maksimalni stepen zaštite vojnog objekta ili prostora,
- da potrebe za fizičkim obezbeđenjem, odnosno broj vojnika na straži svedu na minimum (patrola, grupa za intervencije).

U uslovima povećane opasnosti od terorističkih akcija ili neposredne ratne opasnosti, zaštita prioritetnih objekata, kao što su: skladišta municije, skladišta goriva, komande jedinica, centri veze, vojni aerodromi, lokacije razmeštaja raketnih sistema i sl. može biti dovedena u pitanje zbog propusta

i nepovoljnog uticaja ljudskog faktora. Takvi problemi mogu se izbeći korišćenjem elektronskih sistema. Iskustva u nekim inostranim armijama pokazala su da opasnost ne preti samo od ulaza u štićeni objekat ili prostor spolja, već postoji opasnost od neovlašćenog izlaza iz objekta. Problem postoji ako lica iz fizičkog obezbeđenja ne obavljaju dužnost po pravilu službe. Elektronskim sistemom taj problem se efikasno rešava uspešnim otkrivanjem prolaza kroz štićeni prostor, bez obzira na smer kretanja.

Za razliku od elektronskih sistema koji se koriste za zaštitu civilnih objekata, optimalno rešenje za vojnu primenu (koje obezbeđuju najveći stepen bezbednosti) predstavljaju sistemi za integrisanu tehničku zaštitu. Pod integrisanom zaštitom podrazumeva se zaštita od svih pojava koje mogu dovesti do narušavanja bezbednosti štićenog objekta (protivprovalna zaštita, kontrola ulaza/izlaza osoba, detekcija

požara, pojava opasnih tečnosti i gasova, pasivna i aktivna zaštita, identifikacija uzročnika narušavanja bezbednosti).

Elektronski sistem za integrisanu zaštitu, u suštini, jeste informacioni sistem koji prikuplja, obrađuje, pamti i prikazuje informacije o stanju bezbednosti određenog objekta. Na osnovu tih informacija preduzimaju se mere za fizičku zaštitu štićenog objekta. Elektronski sistem je pouzdaniji i efikasniji od fizičkog obezbeđenja. Stražar može biti dekoncentrisan, umoran, pospan, uplašen, itd., a i ugrožen od napadača, posebno u nepovoljnim atmosferskim uslovima (magla, sneg, kiša i sl.). Elektronski sistem, po pravilu, efikasno deluje u svim vremenskim uslovima i teško može biti ugrožen.

U ovom radu razmatraju se koncepcija, struktura i elementi jednog našeg elektronskog sistema, kao i karakteristike i mogući pravci njegove nadgradnje i mogućnosti vojne primene.

Koncepcija zaštite

Elektronski sistemi za integrisanu zaštitu moraju zadovoljiti vrlo stroge zahteve, a dva osnovna su: prvi — da svaki pokušaj narušavanja bezbednosti objekta (pojedinačni ili grupni upad) mora da detektuje elektronski sistem, a drugi — da šteta koja može zbog toga nastati bude minimizirana upotrebom fizičkih prepreka i grupa za intervenciju.

To znači da fizičke prepreke (ograde raznih tipova) moraju biti tako izvedene da je vreme koje napadač (ili grupa napadača) utroši za njihovo savladavanje, duže od vremena potrebnog da grupa za intervencije (grupa vojnika, patrola i sl.) stigne na mesto napada na štićenom objektu. To se može izraziti sledećom relacijom:

$$T_N \geq T_i \quad (1)$$

gde je:

T_N — vreme potrebno za savladavanje fizičke prepreke, prilazak objektu na kritično rastojanje,

T_i — vreme potrebno grupi za intervencije da stigne do mesta napada koje indicira elektronski sistem.

Analiza vremena T_N , koje je potrebno napadaču da savlada fizičke prepreke, pokazuje da to vreme zavisi od velikog broja parametara, kao što su: broj napadača, kvalitet prepreke, oprema kojom napadač raspolaže, tačka i mesto napada, i sl.

Imajući to u vidu, dominantno je pitanje realizacije elektronskog sistema koji treba pouzdano i blagovremeno da detektuje ugrožavanje bezbednosti štićenog objekta. Civilni objekti se, najčešće, štite samo jednom senzorskom linijom, što za vojne objekte nije prihvatljivo. U zaštiti vojnih objekata prema iskustvima inostranih armija, najčešće se preporučuje upotreba četvorostepenog sistema za detekciju narušavanja bezbednosti štićenog objekta. Koncepcija takvog sistema zaštite prikazana je na primeru objekta koji je prikazan na sl. 1.

Četvorostepeni sistem detekcije sačinjavaju:

— predalarmna linija bezbednosti (sa mogućnošću uključivanja i predalarmne zone);

— alarmna linija postavljena na prvoj ogradi oko objekta (gledano spolja prema objektu);

— linija sigurnosti postavljena na drugoj ogradi oko objekta;

— linija zaštite pojedinih zgrada unutar štićenog objekta, uključujući protivprovalnu unutrašnju zaštitu pojedinih prostorija ili delova zgrada.

Štićeni objekat u primeru sa sl. 1 ima jedan ulaz koji se, takođe, štiti sa tri stepena detekcije, s tim da njima prethodi podsistem za kartičnu

identifikaciju zaposlenih, odnosno posetilaca objekta. Štićeni objekat može imati više ulaza koji se štite po istom principu.

Idući prema štićenom objektu napadač će naići na prvu liniju zaštite, odnosno na predalarmnu liniju elek-

Ako se sa T_p označi vreme potrebno napadaču da prođe kroz predalarmnu zonu i predalarmnu liniju, sa T_a vreme potrebno da pređe put od predalarmne do alarmne senzorske linije i savlada prvu ogradu, i sa T_s vreme potrebno napadaču da pređe put od alar-

Sl. 1 — Konceptija zaštite vojnog objekta

tronskog sistema. Pristup objektu pored predalarmne linije, može biti štićen predalarmnom zonom koja se realizuje postavljanjem senzora u zemljište oko objekta ili u jednoj određenoj zoni. Predalarmna zona omogućava da se detektuje kretanje napadača i odredi njegova putanja kretanja. Iza predalarmne linije postavlja se žičana ograda od bodljikave žice na koju se postavljaju senzori. Na taj način se oko objekta formira druga linija zaštite, odnosno alarmna linija. Iza ograde sa alarmnom senzorskom linijom sledi tzv. linija sigurnosti sa senzorima koji omogućavaju da se precizno definiše mesto i tačka napada na objekat. Iza linije sigurnosti postavlja se, obično, još jedna žičana ograda bez senzora. Pristup ovoj ogradi obično se kontroliše aktiviranjem televizijskih kamera, čime se omogućava vizuelna identifikacija napadača.

mne linije do linije sigurnosti savlađujući drugu ogradu, tada ukupno vreme od pojave alarma do ulaska napadača u štićeni objekat iznosi:

$$T_N = T_p + T_a + T_s \quad (2)$$

Vreme potrebno grupi za intervenciju od trenutka prijema prvog alarmnog signala (iz predalarmne zone ili sa predalarmne linije) do dolaska na mesto, odnosno tačku napada, mora biti:

$$T_i \leq T_p + T_a + T_s \quad (3)$$

Ukoliko je ova relacija zadovoljena, grupa za intervencije može da spreči napadača u njegovim namerama.

Četvrti stepen zaštite predstavlja linija, odnosno podsistem za unutrašnju zaštitu. Time se sprečava da neo-

vlašćene osobe pristupaju zgradama ili prostorijama u određenim zgradama. Na ulaze u zgrade, ili određene prostorije, uz vrata se postavljaju senzori koji generišu alarmne signale u slučaju otvaranja vrata ako se osoba pre ulaska nije identifikovala (korišćenjem identifikacione kartice ili unosenjem broja — lozinke preko tastature elektronske brave).

Pojedine prostorije mogu se štititi senzorima koji detektuju kretanje osoba u štićenom prostoru. U zaštiti vojnih objekata u nekim stranim armijama primenjuju se, pored fizičkih prepreka, i aktivne mere da bi se sprečio pristup štićenom materijalu. U takvim slučajevima, alarmnim signalima se aktiviraju dimne bombe ili bombe sa suzavcem.

Struktura sistema i njegove funkcije

Zahtevani stepen zaštite nekog objekta može se ostvariti ako se pojedinačni sistemi za spoljašnju zaštitu, unutrašnju zaštitu, protivpožarnu zaštitu i dr. međusobno povežu, tj. integrišu u jedinstveni sistem.

Struktura elektronskog sistema za integrisanu tehničku zaštitu prikazana je na sl. 2.

Integrisani sistem sačinjavaju:

1. Računarski podsistem ili centralna alarmna stanica (CAS) koji prikuplja podatke, obrađuje ih, pamti podatke o alarmnim stanjima i upravlja aktivnostima ostalih podsistema.

2. Podsistem za spoljašnju protivprovalnu zaštitu je pasivan sistem koji

Sl. 2 — Struktura elektronskog sistema za integrisanu tehničku zaštitu

CAS-u prosleđuje podatke o alarmnim stanjima kao i informacije o svojoj ispravnosti.

3. Podsistem za unutrašnju zaštitu prosleđuje CAS-u podatke o alarmnim stanjima koja se javljaju pri aktiviranju senzora za unutrašnju protivprovalnu zaštitu. Ovaj podsistem u komunikaciji sa CAS-om otprema podatke o svojoj ispravnosti.

4. Podsistem za pasivnu zaštitu ili izvršni podsistem sačinjavaju ograde, vrata, rampe, barijere i dr. koje se mogu aktivirati (otvoriti ili zatvoriti) komandama koje operator upućuje preko CAS-a. U ovaj podsistem spadaju i drugi izvršni organi koji se aktiviraju preko CAS-a. To su sirene, zvučnici, izvori svetlosti (reflektori) preko kojih se generišu zvučni i svetlosni alarmni signali.

5. Podsistem za aktivnu zaštitu sadrži, pored pomenutih aktivnih elemenata, i elektronske module preko kojih prima komande od senzora. Te komande generišu direktno senzori u alarmnom stanju ili ih upućuje operator preko CAS-a.

6. Podsistem za kartičnu kontrolu ulaza i izlaza osoba u objekte, zgrade ili prostorije, uz korišćenje mehaničkih sredstava (vrata, rampe, barijere), omogućavaju kontrolu osoba koje žele da uđu u određeni prostor. Pod kontrolom se podrazumeva identifikacija preko kartica sa upisanim kodom (najčešće se koristi bar-kod). Očitavanjem identifikacionog koda podsistem sa CAS-om proverava pravo vlasnika da uđe u štićeni prostor, uz istovremeno evidentiranje ulaza/izlaza.

7. Podsistem televizije zatvorenog kruga (TVZK) omogućava identifikaciju stanja na mestu gde je generisan alarm. TVZK omogućava operatoru u CAS-u da podsistem koristi kao senzor.

Elementi sistema

Osnovni elementi jednog našeg elektronskog sistema za integrisanu tehničku zaštitu stacionarnih vojnih objekata prikazani su na slici 3. Centralnu alarmnu stanicu sačinjavaju: personalni računar (PC 486), monohromatski LCD, grafički videoterminal ili grafički kolor CRT video-terminal. Personalni računar je mehanički ojačan, tako da izdržava rad u temperaturnom području od -5°C do $+50^{\circ}\text{C}$. Pojedini podsistemi (sl. 2) priključuju se na personalni računar preko senzorskog terminala (TES) i kartičnog terminala (TEK). CAS sa pomenutim uređajima omogućava:

a) automatski prijem i obradu alarmnih poruka sa senzora (odnosno uređaja TES i uređaja TEK) za spoljašnju zaštitu, unutrašnju zaštitu, pristupnu kontrolu osoba, i dr.;

b) automatsko daljinsko upravljanje elementima za aktivnu i pasivnu zaštitu, kao i ostalim elementima izvršnog podsistema;

c) grafičko i tekstualno prikazivanje i evidentiranje svih funkcionalnih (alarmi, otkazi elemenata u sistemu) i statusnih procesa i podataka koje dobija od pojedinih podsistema;

e) formiranje baze podataka o alarmnim stanjima (liste nepotvrđenih i potvrđenih alarma) i upravljanje bazom podataka;

f) nadgledanje elektronskog sistema za integrisanu zaštitu u smislu kontrole funkcionalnosti i ispravnosti elemenata (otkazi, sabotažne akcije), kao i sistema kao celine.

Neovlašćeno rukovanje računarom sprečava se obaveznim legitimisanjem operatora pomoću numeričke šifre u više nivoa.

SENZORSKI TERMINAL — TES, namenjen je za prijem alarmnih signala, obradu alarmnih signala i upravljanje elementima podsistema izvršnog

Sl. 3 — Elektronski sistem za integrisanu zaštitu stacioniranih objekata i prostora

podсистема, podсистема za aktivnu zaštitu, kao i podсистemom za identifikaciju (televizija zatvorenog kruga). Uređaj TES može da funkcioniše samostalno kao 12-kanalna alarmna centralna stanica. Svi alarmni ulazi prema senzoriima zaštićeni su od prenapona, a linije prema senzoriima od sabotaze, prekida ili kratkog spoja time što se ove pojave automatski dojavljuju CAS-u. Veza uređaja TES sa senzoriima ili senzorskim linijama ostvaruje se preko dvožičnog ekranizovanog kabla dužine do 150 m. Uređaj TES koristi se za rad u stacionarnim uslovima i to ugrađen u zgrade, pričvršćen na spoljnu ogradu ili ukopan u zemlju.

KARTIČNI TERMINAL — TEK koristi se autonomno ili u sistemu integrisane tehničke zaštite, a omogućuje kontrolu kartica (propusnica) sa bar-kodom pri čemu omogućava ili zabranjuje pristup određenom objektu, zgradi ili prostoriji. Bar-kod na kartici

čita se korišćenjem optoelektronskih čitača. Oni se montiraju na zidovima pored ulaza ili vrata ili na posebne stubove unutar objekta. U osnovnoj konfiguraciji jednog integrisanog sistema može se koristiti do 10000 identifikacionih kartica (propusnica). Uređaj TEK omogućava očitavanje lične šifre sa identifikacione kartice sa brojevima kodovanim bar-kodom. Čitač kartica uređaja TEK ima ugrađene LED indikatore koji omogućavaju:

- indikaciju ispravnosti kartice, odnosno dozvoljenog prolaza osobi čija je šifra ispisana bar-kodom na kartici;

- identifikaciju neispravnosti kartice u slučaju pokušaja da se osoba identifikuje korišćenjem neodgovarajuće kartice (sa identifikacionim brojem kome se ne dozvoljava ulaz u objekat).

Čitači kartica povezuju se sa procesorom (mikroračunar) uređaja TEK dvožičnim kablom dužine do 20 m.

Uređaj TEK omogućava komunikaciju sa personalnim računarom centralne alarmne stanice, preko kabla dužine do 1000 m.

SENZORI koji se koriste za detekciju kretanja ili prisustva napadača, funkcionišu na veoma različitim fizičkim principima. Senzori su elementi koji bitno određuju funkcije i performanse sistema za integrisanu zaštitu. Zbog toga se za praktičnu primenu izbor senzora mora obaviti veoma pažljivo, posebno ako se ima u vidu njihov veoma širok asortiman. Izbor senzora za vojnu primenu je relativno ograničen zbog toga što takvi senzori prolaze strogu verifikaciju i atestiranje.

U zavisnosti od primene razlikuju se senzori za spoljašnju i unutrašnju zaštitu. Pregled najčešće korišćenih tipova senzora i njihova klasifikacija prikazani su na sl. 4.

Linijski senzori koriste se za nadgledanje linije ili površine duž neke linije. Najčešće se kao linijski senzori koriste: mikrotalasne senzorske linije ili senzorske linije sa detekcijom promene električnog polja. Takođe se ponekad koriste linijski senzori sa aktivnim infracrvenim zračenjem, zatim senzorske linije sa detekcijom promena

magnetnog polja, kao i senzorske linije sa laserom.

Kod mikrotalasne linije predajnik i prijemnik se postavljaju na rastojanju od oko 100 m. Detekciona površina za različite tipove mikrotalasnih senzora ima različite dimenzije koje se, po potrebi, mogu podešavati.

Princip rada detektora na bazi električnog polja zasniva se na detekciji promene kapaciteta između predajne i prijemne žice, do koga dolazi pri prolazu osobe. Ovaj tip senzora je relativno skup s obzirom na to da zahteva veliki broj mehaničkih delova (stubovi, nosači, žice, i dr.). Detektor promene električnog polja koristi radnu frekvenciju od 10 kHz, tako da je ovaj tip senzora osetljiv na lažne alarme do kojih može doći usled uticaja smetnji. Jednom senzorskom linijom, na bazi promene električnog polja, može se štititi linija dužine do 150 m.

Laserska senzorska linija, u poređenju sa mikrotalasnim senzorom, nije osetljiva na radarsko zračenje. Laserski zrak nije moguće ometati elektromagnetnim poljem. Laserska senzorska linija je osetljiva na pojavu guste magle, jakog snega ili kiše.

Senzorska linija koja se zasniva na principu promene magnetskog polja (u

Sl. 4 — Tipovi senzora

koje ulazi osoba) ima slične prednosti i nedostatke kao detektor promene električnog polja.

Senzorska linija sa aktivnim infracrvenim (IC) senzorom, zavisno od podešavanja nivoa osetljivosti, može detektovati osobu koja prilazi liniji, odnosno kada prolazi kroz IC liniju. IC senzorska linija najčešće se koristi za zaštitu ulaza u objekte. IC senzor je osetljiv na gustu maglu.

Mikrotalasna, laserska i IC senzorska linija osetljive su na uticaj žbunja, trave i drugih prepreka duž linije zaštite.

Senzori postavljeni na ogradi detektuju šumove i signale koji se javljaju pri mehaničkom delovanju (penjanju, sečenju, pomeranju) na ogradu. Problem predstavljaju udari vetra koji mogu izazvati šumove i lažne alarme. Da bi se to izbeglo, pre postavljanja senzorskih linija na ogradu ona mora biti dobro učvršćena i osigurana od vibracija na vetru. Na različitim tipovima ograda može se koristiti više tipova senzora. Kod nas se koristi senzor na principu detekcije vibracija DVD. Radi na principu detektovanja vibracija žičane ograde (pletena žica) na koju se postavlja. Detektori mehaničkih vibracija su pasivni senzori koji su konstrukciono tako izvedeni da reaguju na vertikalno usmerene vibracije, a na horizontalne ne reaguju.

Time je značajno izbegnut uticaj vibracija izazvanih vetrom ili drugim uzročnikom horizontalnog kretanja. DVD se sastoji od elektronskog modula za obradu signala i dve linije detektora vibracija. Linija detektora vibracija sadrži 25 kapsula (vodonepropusna kućišta u koja su ugrađeni elektrodinamički senzori — detektori vibracija) međusobno povezanih ekranizovanim kablom. Kapsule se montiraju na žičanoj ogradi, a mogu se ukopavati u zemljištu na dubini do 20 cm. Osetljivost DVD na vibracije je jednaka po celoj dužini

štićenog prostora (bez nepokrivenih zona). DVD je zaštićen od nedozvoljenih intervencija (sabotaža) na njegovim sklopovima i instalacijama.

Na ograde se, takođe, mogu postavljati triboelektrični detektori TED. Ovaj tip senzorske linije pokušaj prelaza detektuje na principu triboelektričnog efekta u detektorskom kablju postavljenom na žičanoj ogradi. Mehaničke vibracije žičane ograde (izazvane penjanjem osobe ili sečenjem žice) u detektorskom kablju, pretvaraju se u električne signale. Obraduju se u elektronskom modulu i preko senzorskog terminala otpremaju centralnoj alarmnoj stanici (CAS). Elektronski modul konstrukciono je tako izveden (ugrađen u kutiju) da generiše alarm pri pokušaju otvaranja kutije u koju je ugrađen. TED generiše alarmni signal pri pokušaju penjanja, sečenja žice, preskakanja i drugim načinom savladavanja ograde. Zaštićen je od nedozvoljenih intervencija na sklopovima i instalacijama, a neosetljiv je na prolaze malih životinja, ptica i sl. Osetljivost TED-a na vibracije jednaka je po celoj dužini žičane ograde, odnosno nema nepokrivenih zona.

Pored pomenutih tipova senzora na ograde se postavlja tzv. kablovski senzor, koji po celoj dužini prima akustičke signale koji se generišu penjanjem ili sečenjem žičane ograde. Ovaj tip senzora funkcioniše kao mikrofoni.

Senzori koji se postavljaju (ukopavaju) u zemlji veoma su osetljivi na uticaje okoline (seizmički šum, struktura zemljišta, vlažnost, uticaj atmosfernih tonalnih pobuda i dr.). Zbog toga se ovi senzori koriste samo u kombinaciji sa drugim tipovima senzora. Ovi tipovi senzora (elektroakustički, piezoelektrični, senzori promene pritiska, kablovski senzori) reaguju na kretanje pešaka i vozila tako što generišu alarmne signale. Primena ovih tipova senzora povezana je sa problemom obezbeđenja zahtevane osetljivosti i površine koja se mora »pokrivati«, a i sa

problemom sastava zemljišta, odnosno brzinom prostiranja talasa nastalih kretanjem pešaka i vozila.

Za zaštitu ulaza u prostorije (vrata, prozori) koristi se nekoliko tipova senzora, kao što su: detektori loma stakla-DLS, magnetni prekidači, elektronske brave, mreža provodnika («otpor-na» žica), kablovski (žičani) mikrofon.

DLS senzor postavlja se na staklu prozora, a detektuje frekvenciju zvučnog signala koji nastaje lomljenjem stakla. Bistabilni magnetni prekidači detektuju položaj prozora ili vrata, odnosno indiciraju da li su prozor ili vrata (na koje se postavljaju) otvoreni.

Mreža od provodne žice sa odgovarajućom elektronikom, koja detektuje promenu njene otpornosti, generiše alarmni signal u slučaju sečenja žice na mestu gde je postavljena.

Za unutrašnju zaštitu prostorija koriste se senzori koji otkrivaju kretanje osoba ili nekih objekata u štićenom prostoru. Mikrotalasni ili ultrazvučni detektori kretanja utvrđuju veličinu Doplerovog pomaka frekvencije emitovanog signala i signala koji je reflektovan od osobe koja se kreće. Pasivni IC senzor pri radu meri toplotnu energiju u štićenom prostoru i to koristi kao referentni podatak sa kojim upoređuje sve nastale toplotne promene. Pri ulasku osobe u štićeni prostor, toplota koju zrači telo remeti početno »snimljeno stanje«, što registruje senzor koji generiše alarmni signal. Alarmni signal se prosleđuje prema senzorskom terminalu koji obrađuje alarmne signale i upravlja nekim od elemenata izvršnog podsistema (uključuje sirenu i reflektor ili naprave za aktivnu zaštitu). Podatke o alarmu senzorski terminal prosleđuje centralnoj alarmnoj stanici koja ih registruje, pamti, prikazuje i generiše određene upravljačke aktivnosti. Pasivni IC senzori prevashodno su namenjeni za zaštitu unutrašnjeg prostora, a u slučaju montaže na otvorenom

prostoru moraju se zaštititi od meteoroloških padavina i direktnog uticaja sunca.

Mikrotalasni i ultrazvučni senzori kretanja reaguju na male leteće insekte, kao što su leptiri koji lete u blizini predajnika i prijemnika. Ostali izvori smetnji mogu biti jaka strujanja vazduha i kretanje objekata, kao što je pomeranje zavesa na prozorima i sl. Sijalica kao izvor toplotne energije kada se uključuje ili isključuje može ometati IC pasivni senzor kretanja. Pomenute smetnje, koje mogu delovati na pojedine tipove senzora za unutrašnju zaštitu, često ne mogu biti otklonjene. Zbog toga se senzori koji se baziraju na različitim fizičkim principima detekcije, ugrađuju u ista kućišta, pa se formira senzor (na primer dualni mikrotalasni-pasivni IC) koji reaguje samo ako oba tipa senzora detektuju kretanje u štićenom prostoru.

Senzori za spoljašnju zaštitu posebno su osetljivi na lažne alarme koji nastaju usled smetnji izazvanih uticajima okoline. Pod tim se podrazumevaju klimatske promene (oluja, grmljavina, snežne padavine, kiša, magla i dr.) koje se ispoljavaju kao akustične i elektromagnetske smetnje. Oba pomenuta tipa smetnji imaju veoma važnu ulogu u projektovanju i funkcionisanju elektronskih sistema za zaštitu vojnih objekata. Teška borbena i neborbena vozila (transporteri, tenkovi i dr.), vazdušni saobraćaj na aerodromima, snažni radarski sistemi, nepovoljno utiču na funkcionisanje elektronskih sistema za tehničku zaštitu, pa se taj uticaj mora uzeti u obzir kada se projektuju elementi sistema, posebno podsistemi za spoljašnju protivprovalnu zaštitu, odnosno kada se vrši izbor tipova senzora koji će se primeniti. Projektanti sistema za tehničku zaštitu mogu odabrati elemente i korektno primeniti elektronski sistem za tehničku zaštitu samo ako poseduju ekspertsko znanje o tome kako funkcionišu

različiti sistemi i senzori u konkretnim uslovima okoline.

Da bi se to ostvarilo, potrebno je:

- precizno definisati projektni zadatak i zahteve koje elektronski sistem treba da zadovolji;

- proceniti uslove rada sistema u konkretnom okruženju;

- definisati metode ispitivanja karakteristika sistema u realnim uslovima rada;

- obaviti proveru karakteristika sistema u dugotrajnom radu.

Neka iskustva iz operativne upotrebe sistema pokazala su da izbor tipova i instaliranje senzora, prema karakteristikama koje deklarišu proizvođači, može dovesti do grešaka i problema u eksploataciji. Razlog za to jeste u tome što se ne uzimaju u obzir specifični uslovi primene i mogući uticaji akustičkih, elektromagnetskih i drugih smetnji.

Imajući u vidu ove probleme kod nas je uspešno realizovan računarski ekspertni sistem [1] koji omogućava:

- pomoć u projektovanju elektronskih sistema za integrisanu zaštitu i izradu tehničke dokumentacije;

- simulaciju projektovanog ili realizovanog sistema tehničke zaštite radi analize funkcionisanja u realnim uslovima. Pri tome se programski simuliraju alarmna stanja ili otkazi sistema i donose zaključci o ponašanju i kvalitetu sistema za integrisanu zaštitu, analizom »odgovora« sistema na pobude i otkaze;

- proračun pouzdanosti sistema i analizu njegove efikasnosti u poređenju sa efikasnošću i troškovima zaštite objekta kada se on fizički obezbeđuje;

- obučavanje kadrova za rukovanje, osnovno i tehničko održavanje elektronskog sistema za tehničku zaštitu.

Ideja je da se primenom metoda veštačke inteligencije [1], odnosno ek-

spertnog sistema sa bazom znanja, efikasno reše problemi optimalnog projektovanja sistema za integrisanu tehničku zaštitu, kao i drugi problemi vezani za njegovo funkcionisanje i održavanje (analiza uticaja otkaza, pouzdanost, efikasnost, ekonomičnost, obuka u rukovanju i održavanju).

Primena elektronskih sistema u zaštiti vojnih objekata

Primena elektronskog sistema u zaštiti konkretnog vojnog objekta ili prostora mora biti dobro osmišljena i prostudirana. Pod osmišljavanjem se podrazumevaju aktivnosti koje moraju obaviti organi, odnosno jedinice zadužene za bezbednost konkretnog objekta. To se, pre svega, odnosi na procenu ugroženosti, tj. ko i na koje načine može narušiti bezbednost objekta. Ova aktivnost se u literaturi često zove studija pretnji konkretnom objektu. Na osnovu procene bezbednosti, odnosno zaključaka iz studije pretnji, treba izraditi (uz pomoć budućeg projektanta sistema) detaljne tehničke i projektne zahteve za elektronski sistem, na osnovu kojih će projektant izraditi projekat. Izrađeni projekat podleže strogoj stručnoj recenziji i overi nadležnog organa. Elektronski sistem izrađen po projektu mora biti detaljno ispitan i proveren u realnim uslovima u dugotrajnom radu, pre puštanja u eksploataciju.

Kada je reč o primeni elektronskih sistema za integrisanu tehničku zaštitu vojnih objekata, nameće se pitanje poverljivosti posebno kada se radi o prioritetnim objektima za koje se zahteva najviši stepen bezbednosti. Sigurno da podaci o elementima sistema kao što su senzori, mikroračunari, terminali i sl. ne predstavljaju tajnu. Ti podaci su kod nas i u svetu svima dostupni [2].

U svetu se štite (smatraju se poverljivim) projektni zahtevi, projekat, kao i konkretna realizacija elektronskog sistema. Drugim rečima, tajna je kako je i čime konkretni objekat zaštićen. Mora se pretpostaviti da sistem, kojim se neki objekat štiti, može biti osmatran, ometan, obmanjivan lažnim alarmima, odnosno izložen sabotazi. Konkretni elektronski sistem ne bi smeo da ima slaba mesta osetljiva na pomenute aktivnosti, a ako ih ima, ona se moraju fizički štititi stražom, a podaci o tome takođe predstavljaju tajnu. Veoma je važno da elektronski sistem bude testiran na lažne alarme, obmanjivanje, ometanje, sabotажne aktivnosti i sve ono što može uticati na njegovu pouzdanost, odnosno raspoloživost. Ipak, pred savremene elektronske sisteme za zaštitu vojnih objekata postavlja se zahtev da moraju omogućiti otkrivanje napadača (jednog ili grupe) i uz pretpostavku da on raspolaze svim podacima o elektronskom sistemu kojim se objekat štiti. Drugim rečima, elektronski sistem uvek mora obezbediti informaciju o tome na koji je način ugrožena bezbednost štićenog objekta. Pri tome se fizičkim preprekama napadač primorava da »troši« vreme i time stvaraju uslovi da grupa za intervencije stigne u ugroženu zonu i tako spreči moguću štetu.

U konkretnoj primeni elektronskih sistema za zaštitu vojnih objekata pažnju zaslužuju dva pitanja: koncepcija sistema i dostupnost (mogućnost opremanja) uređaja, opreme i elemenata za realizaciju sistema.

Koncepcija zaštite prethodno je objašnjena. U konkretnoj primeni mora se ići na maksimalni (čtetvorostruki) stepen zaštite. Pored toga, ukoliko ekonomske mogućnosti investitora to dozvoljavaju, sistem treba udvajati. Po pravilu, udvajaju se centralne alarmne stanice, posebno ako se radi o velikim objektima. Uz svaku stanicu stacioni-

ra se po jedna grupa vojnika za intervencije. Obe centralne alarmne stanice međusobno razmenjuju podatke, tako da su isti podaci prisutni na dva mesta. Takođe, udvajaju se senzori na pomenutim senzorskim linijama. U primeni senzora važi pravilo da se u pojedinim linijama zaštite moraju koristiti senzori koji funkcionišu na različitim fizičkim principima. Na primeru objekta koji je prikazan na sl. 1, to bi, praktično, značilo:

— da predalarmnu liniju treba realizovati korišćenjem mikrotalasnih senzora koja se može udvojiti laserskom senzorskom linijom;

— da se alarmna linija može realizovati korišćenjem kablovskog senzora ili tribo-kabla, a udvajati senzorskom linijom tipa DVD;

— da se linija sigurnosti može realizovati senzorom na principu električnog polja, a alternativno linijom koja se bazira na detektoru promene magnetskog polja;

— da se četvrti stepen zaštite mora realizovati udvajanjem senzora, na primer, upotrebom dualnih mikrotalasnih i pasivnih IC senzora, itd.

Udvajanjem nekih elemenata sistema povećava se pouzdanost funkcionisanja sistema i, praktično, onemogućava da bude ometan ili obmanut.

Opremanje elementima, uređajima i opremom za tehničku zaštitu moguće je iz domaće proizvodnje. Uspešno obavljen razvoj i pripremljenost proizvođača [2] omogućavaju da se u zaštiti koriste savremena tehnička rešenja.

Zaključak

Elektronski sistemi za integrisanu tehničku zaštitu dobijaju sve veći značaj u zaštiti vojnih objekata s obzirom na to da mogu ostvariti maksimalni stepen bezbednosti vojnog objek-

ta. Njihovim uvođenjem umanjuju se potrebe za fizičkim obezbeđenjem, odnosno broj vojnika na straži svodi se na najmanju meru. Kod nas postoje

mogućnosti opremanja elementima, uređajima i opremom za tehničku zaštitu iz domaćeg proizvodnog programa.

Literatura:

[1] Kantardžić, M., Jevtović, M.: A COMPRENSIVE ENVIRNMENT FOR COMPUTER AID IN TECHNICAL SECYRITY SISTEM DESIGN; Proceedings of the International Conference in Vienna, Austria, 1990. str. 417—420.

[2] Prospektni materijali za elemente, opremu i uređaje elektronskih sistema za tehničku zaštitu, Ei HOLDING Co. DD, Profesionalna elektronika iz Niša.