LXIX Konferencija ETRAN, Čačak, 9 - 12. Jun 2025.

Internet inteligentih uređaja tehničke bezbednosti u kazneno-popravnim ustanovama u podršci procesu odlučivanja u bezbednosno incidentnim situacijama

Kristijan Đujić
Kazneno-popravni zavod za maloletnike
Valjevo, Srbija
kristijan.djujic@gmail.com i ORCID
0009-0005-1846-3390

Martin Matijašević
Poslovni i pravni fakultet
Univerzitet MB
Beograd, Srbija
martin.matijasevic@yahoo.com i ORCID
0009-0006-5840-7446

Radovan Radovanović
Kriminalističko-policijski univerzitet red
Beograd, Srbija
radovan.radovanovic@kpu.edu.rs i
ORCID 0000-0001-7302-8328

Saša Milić
Elektrotehnički Institut Nikola Tesla,
Faculty of diplomacy and security
Beograd, Srbija
sasa.milic@yahoo.com i ORCID 0000-
0001-5757-3430

Abstract*—U radu se analizira internet inteligentnih uređaja tehničke bezbednosti u ustanovama za izvršenje krivičnih sankcija u podršci procesu odlučivanja u bezbednosno incidentnim situacijama. Ustanove za izvršenje krivičnih sankcija po svojoj funkciji su mesta sa visokim rizikom od bezbednosno incidentnih situacija. Inteligentni uređaji tehničke bezbednosti su strukturisani u uređaje za video nadzor i perimetrijsku zaštitu, uređaje za održavanje veze, uređaje za otkrivanje i prepoznavanje nedozvoljenih metalnih predmeta, sisteme za kontrolu pristupa i idetifikaciju, sisteme detekcije požara i sisteme mehaničke zaštite, čijom integracijom sistem tehničke bezbednosti čini funkionalnu celinu. Integracija ovih sistema treba da pomogne strategijskom i top nivou bezbednosnog menadžmenta u procesu odlučivanja u uslovima bezbednosno incidentnih situacija.

Ključne reči—zavodi, tehnički, bezbednost, inteligentni, sistem, incidenti

I. Uvod

Pored ljudskog faktora koji je dominantan i ključan u sistemu obezbeđenja ustanova za izvršenje krivičnih sankcija koje su po svojoj osnovnoj funkciji ustanove sa visokim bezbednosnim rizikom, održavanje potrebnog nivoa bezbednosti nemoguće je ostvarivati bez tehničke komponente sistema obezbeđenja. U savremenom i izmenjenom bezbednosnom kontekstu ustanove za izvršenje krivičnih sankcija suočavaju se sa brojnim bezbednosnim izazovima, rizicima i pretnjama, kakva je danas npr. Covid-19, koje zahtevaju tretman i integrisani odgovor u sinergiji između fizičke i tehničke komponente sistema obezbeđenja [1].

Može se konstatovati da je bezbednosni problem ustanova za izvršenje krivičnih sankcija kompleksan, te i njegova zaštita mora da ima takav koncept, koji bi se sprovodio kroz integraciju različitih bezbednosno-tehničkih sistema. Stepen i način integracije zavise od tehničkih i bezbednosnih karakteristika sistema i vrste prostora i objekta na kome se primenjuju. Značajnu ulogu u integraciji imaju proceduralno-bezbednosni i tehnološki postupci koji se sprovode u štićenom prostoru. Uzimajući u obzir karakter objekata ovih ustanova, pozicije pojedinih komponenti elektronske zaštite treba da budu uočljive i da već svojim prisustvom odvraćaju od pokušaja realizacije nekog oblika bezbednosne pretnje, tako što se kod osuđenika razvija osećaj da se nad njima vrši permanentni nadzor. Osećaj neprekidne prisutnosti bezbednosnih struktura u afirmativnom smislu značajan je i sa pozicija samog obezbeđenja, uključujući i sve zaposlene u ovim ustanovama. Sa druge strane, imajući u vidu sve ljudske karakteristike i prirodnu odbojnost prema kontroli, sistemi moraju da budu maksimalno automatizovani kako bi se izbegle nepotrebne ručne manipulacije korisnika.

U teoriji postoji šest pitanja, kojima trebaju da se vode kreatori politike bezbednosti u procesu njenog stvaranja [2]. Koga štititi? Koje vrednosti štititi? Koliki je željeni stepen bezbednost i kolika je njegova cena? Koji su rizici, izazovi i pretnje od kojih se treba čuvati? Kojim sredstvima se štititi? Koliko dugo se štititi? Ova pitanja su posebno složena za kreatore sistema izvršenja krivičnih sankcija, jer je reč o ustanovama koje funkcionišu u specifičnom i dinamičnom okruženju. Zbog svega navedenog u sistemu izvršenja krivičnih sankcija razvijena je posebna komponenta bezbednosti.

II. Koncept dinamičke bezbednosti u zatvorima

Bezbednost i sigurnost za sve osobe u zatvoru kamen je temeljac delotvornog i humanog zatvorskog režima. Spoljna bezbednost (sprečavanje bekstva) i unutrašnja sigurnost (sprečavanje nereda) najbolje se obezbeđuju izgradnjom pozitivnih odnosa između zatvorenika i osoblja (koncept „dinamičke bezbednosti“) [3].

Dinamička bezbednost podrazumeva znanje o tome šta se dešava oko vas i stvaranje sigurnih uslova za život lica lišenih slobode i rad zaposlenih u zatvoru [4]. Dinamička bezbednost u zatvorskom okruženju ima tri osnovna elementa sigurnosti: 1) fizički (zidovi, ćelije ili spavaonice), rešetke, ograda, kapija, svetla, videonadzor i alarmni sistem; 2) proceduralni (sprovođenje, prebrojavanje, pretres zatvorenika, posetilaca, osoblja i unutrašnjih i spoljašnjih površina, patroliranje, otključavanje i zaključavanje lica lišenih slobode i 3) lični odnosi i stav prema drugima, obavljanje zadataka

ISBN 978-86-6200-032-3 ©2025 AM & ETRAN
https://doi.org/10.69994/69E25057

Ovaj rad podleže licenci CC BY-NC-ND 4.0 International

efikasnog zatvorskog službenika [5]. Četiri dodatna elementa dinamičke bezbednosti su:Dobri odnosi između zatvorenika, osoblja, službi i spoljašnjih agencija i ustanova za sprovođenje zakona i svih posetilaca koji posećuju ustanovu;Konstruktivan režim u kome je licima lišenim slobode data mogućnost da uče ili unapređuju socijalne veštine, da razmisle o svom ponašanju i pripreme za puštanje na slobodu. Bezbedno okruženje koje pruža ličnu i opštu sigurnost osuđenicima da žive i osoblju da radi, ne zaboravljajući pri tome potrebu da se zaštiti javnost držeći u zatvoru osobe koje je sud osudio za krivična dela. Bilo šta što smanjuje želju za bekstvom, potreba da se obezbedi režim u kome u svakom momentu znamo šta se dešava, sigurno okruženje koje pružamo osuđeniku u kojem može napredovati kroz kaznu prema otpustu, dajući mu koristan i svrsishodan radni angažman, održavajući familijarne veze i omogućujući im zdrav život tokom boravka u zatvoru kroz fizičke aktivnosti i odgovarajuću ishranu i na kraju kroz podsticanje osoblja da postupa prema osuđenicima sa poštovanjem i razumevanjem kad god je to moguće [6].

Sa aspekta bezbednosnih rizika u sistemu izvršenja krivičnih sankcija, mogu se javiti sledeći rizici: organizaciono-arhitektonske prirode (prenaseljenost zatvora, neadekvatna arhitektonska rešenja objekata), rizici iz domena socijetalne bezbednosti (izražen jak uticaj neformalnog osuđeničkog sistema u velikim kazneno-popravnim zavodima, nepovoljna kriminološka struktura osuđenih u odnosu na tipove zavoda) [7], rizici iz bezbednosti tehničkih sistema (neadekvatna opremljenost ustanova u bezbednosnom i tehničkom smislu, neispravnost uređaja i instalacija) [8], rizici iz oblasti ostvarivanja prava lica lišenih slobode [9], rizici od disciplinskih prestupa i rizici iz oblasti održavanja reda i bezbednosti. Kod nekih osuđenika ideja bekstva je prisutna od momenta dolaska u zatvor bez obzira na stepen obezbeđenja institucije u kojoj se nalaze. Oni stalno razrađuju planove za bekstvo što vremenom stvara posebne psihološke mehanizme odbrane i prilagođavanja na sve frustracije koje neminovno boravak u zatvoru donosi sa sobom, pa se javljaju rizici od bekstava [10].

Usled beskućništva, neuhranjenosti i intravenskog uzimanja droge, brojni osuđenici nose faktore rizika za jednu ili obe infekcije [11]. Stopa samopovređivanja i samoubistava u zatvoru je četiri puta veća od stope samoubistava u opštoj populaciji, pa se javljaju i ovi rizici [12]. Prisutni su i rizici od terorizma, talačkih situacija, pobuna, vandalizma, podmetanja požara i sabotaža [13], kao i rizici kod sprovoda lica lišenih slobode [14]. Nakon definisanja elemenata potencijalnih rizika i pretnji, slede preporuke u cilju efikasnog načina sprečavanja istih, sa mogućnošću kontrolisanja incidentnih situacija, i to kroz [15]: identifikovanje učesnika u sistemu zaštite objekata, lica i materijalnih dobara u njemu, sa predloženim načinom delovanja tokom redovnih aktivnosti i u incidentnim situacijama, definisanje namenskih tehničkih sredstva i sistema za zaštitu lica i materijalnih dobara, definisanje minimalnih tehničkih, bezbednosnih i organizacionih principa na kojima će se zasnivati rešenja sistema tehničke i organizacione zaštite, kao i za integraciju bezbednosnih tehničkih sistema.

III. SISTEM TEHNIČKE BEZBEDNOSTI U ZATVORIMA

Struktura sistema u ovom modelu obezbeđenja Kazneno popravnog zavoda zatvorenog tipa. Uređaji za video nadzor i perimetrijsku zaštitu (alarmi za obezbeđenje objekata i prostora druge vrste zaštite), uređaji za održavanje veze, uređaji za otkrivanje i prepoznavanje nedozvoljenih metalnih predmeta, sistem za kontrolu pristupa i idetifikaciju pomoću biometrijskih i drugih čitača, mehanička zaštita, sistem detekcije i dojave požara. Sistemi za tehničku zaštitu se integrisani u jednu radnu celinu. Poslovi nadzora pomoću sistema za tehničku bezbednost u zavodu obavljaju se neprekidno. Sistemima za bezbednost mogu rukovati operateri koji su adekvatno obučeni za rad sa instaliranim sistemima u zavodu. U zavodu pored Operativnog centra nadležnost poslova nadzora pomoću sistema za tehničku bezbednost obavljaju se u Operativnim podcentrima u skladu sa dodeljenim pravima na osnovu zona nadležnosti koje definiše Plan za obezbeđenje. Operativni centar ima nadležnost nad svim podcentrima. Korisnička prava nad sistemima za bezbednost u Operativnom centru dodeljena su operaterima da mogu vršiti sledeće radnje:

Sistem video obezbeđenja - pregled svih kamera u sistemu, premotavanje događaja na svakoj kameri, upotrebu pametnih zidova za video obezbeđenje koji je povezan sa svim bezbednosnim sistemima. Sistem kontrole pristupa, dojave požara, centralnog upravljanja, radio veze, komunikacije. Ureađaji koji služe za otkrivanje i prepoznavanje nedozvoljenih predmeta; metal detektorska vrata, skener. Sistem kontrole pristupa - pregled događaja prilikom korišćenja personalizovanih kartica u okviru objekta, u slučaju neautorizovanog očitavanja kartice, radnja se prikazuje na sistemu za video obezbeđenje.

Sistem radio veze - praćenje 8 komunikacionih grupa koje su konfigurisane u okviru zavoda. Obraćanje svim korisničkim grupama (pojedinačno-privatno, grupno, više grupa, svi), Preusmeravanje privatnih poziva, rukovanje sistemom prilikom panik aktivacije (panik dugme, man-down) radnja se prikazuje na sistemu za video obezbeđenje, otvaranje zvučnika korisnika prema delegiranim pravima. Sistem za komunikaciju - nadležnost nad svim intefonskim uređajima u zavodu, Snimanje komunikacije ukoliko za to postoji odobrenje, SOS aktivacija za vanredne događaje-radnja se prikazuje na sistemu za video obezbeđenje, pozivanje svih IP telefona u objektu, spoljna telefonska veza, rukovanje razglasnim sistemom u okviru zavoda. Sistem detkcije i dojave požara; Praćenje sistema prilikom aktiviranja alarma (ručni-automatski) radnja se prikazuje na sistemu za video obezbeđenje.

Sistemima za bezbednost mogu rukovati operateri koji su adekvatno obučeni za rad sa instaliranim sisitema u zavodu. U zavodu pored operativnog centra nadležnost poslova nadzora pomoću sistema za tehničku bezbednost obavljaju se u operativnim podcentrima u skladu sa dodeljenim pravima na osnovu zona nadležnosti koje definiše Plan za obezbeđenje. Operativni centar ima nadležnost nad svim podcentrima. Korisnička prava nad sistemima za bezbednost u Operativnom podcentru dodeljena su operaterima da mogu i autonomno

vršiti prethodno pomenute radnje. Informatička bezbednost se zaniva na svojoj lokalnoj mreži, preko koje se ostvaruju sva informatičko tehnička prava. Mreža je zaštićena od spoljašnih upada i adekvatnim antivirusnim programima. Zabranjena je upotreba svakog vida korišćenja prenosivih nosača memorija (CD, USB, Harddrive) na način da je hardverski isključena mogućnost korišćenja (osim na mestima za koje postoji potreba da se isti koriste i koji su registrovani). Zabranjeno je unošenje bez odobrenja i kontrole stručnog lica svakog vida nosača memorije i drugih informatičko tehničkih komponenti [16].

IV. Sistem video nadzora u zatvorima

Sistem video nadzora treba realizovati u kolor tehnologiji visoke rezolucije. Imajući u vidu potrebu za instalacijom većeg broja kamera, primeniti IP tehnologiju u okviru posebne namenske računarske mreže i koristiti sa svim benefitima koje nudi ova tehnologija, kao što je generisanje alarma prema različitim kriterijumima:

-alarm zasnovan na pokretu - VMD (Video Motion Detection) ili video detekcija pokreta, koja definiše aktivnosti analiziranjem podataka u slučaju promene osvetljenosti na unapred definisanom delu snimane scene (značajano za video nadzor reona perimetra i pojedinih otvorenih i zatvorenih prostora u samom objektu KPZ-a);

-alarm u audio domenu, bilo da se pokrene snimanje po audio detekciji na samoj kameri, ili da se u jednom ili u oba smera odvija audio-video komunikacija na potezu snimanja scena - radna stanica/serverska radna stanica (npr. na nivou mrežnog videa, gde je integrisana i audio opcija, osoblje u operativnom centru u mogućnosti je da čuje komunikaciju duž perimetarskog zida i da npr. komunicira sa beguncima), moguća je i varijanta nasnimavanja audio upozorenja po audio detekciji ili detekciji pokreta;

-inteligentna analiza pokreta, u cilju otkrivanje vozila, ljudi i drugih objekata koji se kreću u zabranjenoj zoni ili u zabranjenom smeru, kretanje neprilagođenom brzinom uključujući i zaustavljanje vozila na nedozvoljenom mestu;

-detekcija objekta podrazumeva prepoznavanje vozila i osoba, ili ljudi i životinja u aplikacijama za nadzor perimetra, sa sofisticiranom mogućnošću prepoznavanja boja i oblika;

-analiza statičkih objekata pokreće alarm ukoliko se detektuje ostavljeni objekat, a koji se do tada nije nalazio u vidnom polju kamere, ili pak pomeranje objekata od kojih se to ne očekuje,

-nadzor zagušenja nekog prolaza ili prostora gde se određenim alarmnim signalom centru dojavljuje da se u određenom prostoru nalazi previše ljudi ili nekih objekata;

-postavljanje zamišljenih barijera (iscrtavanje linije barijere na videu pojedine kamere), čije uzurpiranje bi bilo dojavljeno kao alarm;

-funkcija brojanja ljudi može biti veoma korisna u slučaju kontrole pojedinih prolaza (npr. broj ljudi koji je ušao, a kasnije i napustio industrijski deo KPZ-a), i može biti veoma važan podatak kao evidencija brojnog stanja osuđenika, što je u uskoj vezi sa pokušajima bekstva.

V. Sistem perimetarske zaštite u zatvorima

Sistemom perimetarske zaštite treba obezbediti narušavanje integriteta perimetarskog zida ili ograde KPZ-a, u spoljnoj i unutrašnjoj zoni perimetra. Sistem perimetarske zaštite, kojim treba štititi spoljni pojas perimetarske linije ustanova, pripada grupi sistema elektronske zaštite koji obezbeđuju granični, otvoreni pojas interesnog objekta (engl. outdoorsecurity), a u cilju rane dojave ili upozorenja na pojavu bezbednosne pretnje, često sa veoma udaljenih i/ili nepristupačnih delova perimetra. Ovim se otvara mogućnost blagovremenog reagovanja, uz minimalni rizik po bezbednosne strukture, ljude i sam objekat [17]. U okviru perimetarske zaštite, a koja se tiče delova zida ustanova koji prodire u dubinu kompleksa, uključujući i krovne konstrukcije koje se građevinski nastavljaju na ovaj zid, isto tako je potrebno predvideti zadovoljavajući oblik elektronske zaštite, a koji bi bio raspoloživ da detektuje pokušaje bekstva, upada i sl. Ovakvim prostorima odgovaraju tehnička rešenja koja definišu tzv. „sterilne zone" i „elektronske barijere", koje se pozicioniraju između dve fizičke barijere i duž nedozvoljene linije pristupa (npr. Blizu unutrašnje granične linije zatvorskog zida), detektujući na taj način pokušaje njihovog premošćenja kao očekivan scenario upada. Na slici 1. dat je opšti primer akcije i reakcije na neki oblik bezbednosne pretnje u objektu kao što je KPZ, sa najpribližnijim opisom mogućeg scenarija:

-detekcija senzorskog tipa u zoni perimetra, koja podrazumeva spregu nekog oblika perimetarske zaštite i televizije zatvorenog kruga (CCTV);

-eventualnu detekciju i drugih oblika akcidenata (unutar zatvorenog dela KPZ, događaji na kontrolisanim prolazima u sistemu kontrole pristupa, problemi na punktovima za kontradiverzioni pregled i dr.), gde su oni opisani kao spoljni podsistemi. Podaci sa naznačenih senzorskih periferija se prikupljaju, kontrolišu i obrađuju, vrši se njihov monitoring, a na osnovu prikaza aktuelne situacije i procene službe fizičko-tehničkog obezbeđenja, operater stupa u komunikaciju sa službom fizičkog obezbeđenja koja u najkraćem vremenskom periodu stiže na mesto akcidenta.

Drugim rečima, princip perimetarske zaštite bazira se na očekivanoj pretnji koja napada tzv. prvu liniju odbrane štićenog objekta, a koja treba potencijalnog počinioca akcidenta (upadača, begunca i sl.):

-u prvi mah da odvrati od pokušaja izazivanja bezbednosnog problema postavljanjem mehaničkih barijera, kapija, ograda, zidova i sl.;

-da detektuje akcident putem adekvatnih senzora, čime se obezbeđuje rano dojavljivanje nedozvoljenog pokušaja ulaza ili napuštanja perimetarskog kruga nadzornom centru (CTO);

-da što više uspori počinioca u pokušaju pristupa ključnim pozicijama i da mu maksimalno produži vreme potrebno za procenu situacije koja prati incident, upotrebom mehaničkih prepreka, audio/vizuelnih alarma i uređaja koji rade na principu vremenskog zatezanja;

-da se u postupku procene nastale situacije nadzornom centru Službe za obezbeđenje proslede pouzdane potvrde generisanog alarma direktnim vizuelnim pregledom ugrožene zone, uvidom u sadržaj kojim raspolaže monitoring centar (CCTV, CTO) i adekvatnim osvetljenjem duž kompletne perimetarske linije;

-da se na nastalu okolnost adekvatno odgovori reakcijom na nivou Službe za obezbeđenje, što predstavlja naznačenu bezbednosnu prednost impliciranu postojanjem tzv. outdoor zaštite. Ukoliko to situacija nalaže, reakcija Službe za obezbeđenje može biti proširena i sadejstvom sa policijskim snagama.

Senzori pokreta su postavljeni spolja da detektuju pokrete pomoću infracrvenih zraka. Sistem može biti aktivan, ako emituje izvor napajanja radi lakšeg otkrivanja, ili pasivan, ako je ograničen na slanje alarma kada dođe do promene temperature ili kretanja. Sistemi detekcije optičkih vlakana koriste se za otkrivanje prisustva pomoću optičkog kabla. Pogodan je za zaštitu ograda i zidova, kao i za pokrivanje velikih perimetarskih proširenja. Zemaljski radarski sistemi zaštite perimetra. To su radari koji detektuju prisustvo ljudi ili vozila na srednjoj udaljenosti (1500 metara) i maloj udaljenosti (700 metara). Pogodni su za upotrebu u izolovanim postrojenjima okruženim poljima i sa otvorenim pristupima koje je teško kontrolisati drugim sistemom. Mikrovalne barijere mogu otkriti potpuno skrivena prisustva i pokrete. Za ovo koristite mikrotalasnu emisiju. Električne ograde - ograda je elektrifikovana i ako neko pokuša da je preseče ili se popne, šalje seriju obaveštenja ili aktivira alarm. Ovaj sistem izaziva strujne udare uljeza, tako da nije dozvoljen u svim zemljama, na primer u Evropi se može raditi samo u kritičnim instalacijama i uz posebne dozvole .

Senzori poremećaja elektrostatičkog polja. Stvaranjem električnog polja, korišćenjem provodnika i uzemljenja, prisustvo se može detektovati kada se to električno polje promeni. Spot senzori vibracija. To je efikasan tip bežičnih perimetarskih alarma. Sastoji se od senzora koji se postavlja u vrata, prozore i druge moguće pristupe. Bežični senzor se aktivira kada detektuje vibracije u vratima ili prozorima i aktivira alarm. Seizmički senzori. Ovi uređaji detektuju vibracije u svom polju delovanja i aktiviraju alarm. Oni ne služe za otkrivanje zemljotresa, već vibracije koje mogu imati više porekla. Moguće upozorenje bi bio pokušaj pljačke putem rupe u zidu za pristup trezoru ili protiv upotrebe termalnih koplja za prolaz kroz čelik ili beton. Kombinujući dve ključne bezbednosne funkcije u jednom vrhunskom proizvodu, Senstar LM100 deluje kao moćno sredstvo odvraćanja od uljeza, otkrivajući ih i osvetljavajući ih na liniji ograde, istovremeno upozoravajući bezbednosni sistem lokacije [19]. Virtuelna ograda/barijera se kreira na osnovu skupa koordinata na geografske oblasti koje su mapirane preko GPS-a ili VPS-a, što [20] omogućava daljinsko praćenje zatvorenika koji su okruženi virtuelnom ogradom. Sigurnost perimetra obezbeđuje bilo koji metod koji ograničava pristup definisanom području, kao što je vojna baza, korporativni kampus, infrastrukturni objekat ili poslovna zgrada. To je prvi sloj odbrane u fizičkom obezbeđenju [24]. Mehanizmi za fizičko obezbeđenje štiti ljude, podatke, komunikaciju, objekte i informacione resurse [21].

VI. Sistem bezprekidnog napajanja

Nestanak mrežnog napona je nepovoljan sa aspekta rada uređaja u sistemu tehničke zaštite, koji ni jednog momenta ne treba da ostanu bez napajanja (serveri, kamere, sistem perimetarske zaštita, centrala kontrole pristupa, interkomunikacioni i videointerfonski sistem, alarmna centrala, računari...). U cilju prevazilaženja takvih situacija, neophodno je predvideti sistem bezprekidnog napajanja (UPS), koga čine uređaji raspoloživi da svim W potrošačima u sistemu tehničke zaštite obezbede bezprekidno napajanje sinusnim naponom nezavisno od kvaliteta raspoložive mreže. Predvideti tzv. ON LINE sistem, gde su potrošači stalno priključeni na potpuno „očišćen" napon, preko invertora. Sistemom bezprekidnog napajanja eliminisali bi se problemi kao što je narušavanje integriteta podataka, rada računara, i uopšte kompletnog sistema integralne tehničke zaštite koji bi u takvim, vanrednim okolnostima ostao operativan. Sistem bezprekidnog napajanja treba da zadovolji sledeći radni režim, koji predstavlja i njegov operativni minimum:

-u normalnom radu, potrošači mrežni napon dobijaju preko invertora, a potreban jednosmerni napon za njegov rad obezbeđuje ispravljač, koji u isto vreme i puni bateriju UPS-a;

-u slučaju nestanka mrežnog napona, zahvaljujući automatskom preusmeravanju napajanja, UPS automatski prihvata opterećenje za potrebe tehničke zaštite sve dok se ne uključi agregat ili ponovo ne uspostavi mrežni napon, čime se sistem vraća u normalni radni režim.

VII. Novoinkorporirano serversko softversko rešenje

Novoinkorporirano serversko softversko rešenje omogućava opciju pametnog video zida u sistemu video nadzora koje daje mogućnosti integracije sa ostalim sistemima tehničke zaštite shodno njihovim tehničkim potencijalima. Pricip rada integracije sistema možemo definisati pravilima na sistemu video nadzora i putem mrežnog protkola drugih sistema tehničke zaštite poslati informaciju sistemu kao alarm. Ovakav vid integracije omogućava da se video nadzor ne prati neprekidno, već da se pažnja usmerava na sistem kada se automatizovano javi alarm nekog od sistema, koji pored opcije automatizacije procesa da se prikaže na pametnom video zidu daje i zvučnu signalizaciju. Sistem zvučne signalizacije se može prilagoditi vanrednom događaju alarma, pa samim tim pripadnik Službe za obezbeđenje u Operativnom centru – dežurnoj službi pri samom zvučnom signalu ima jasnu informaciju koji vanredni događaj je u pitanju pre nego što ostvari uvid sa lica mesta, vanredni događaj se automatizovano prikazuje i u nadležnom podcentrnu za bezbednost, tako da drugi pripadnici Službe za obezbeđenje nemaju saznanja o događaju, već imaju samo oni u čijoj je to nadležnosti. Ovakav vid integracije sistema koji se projektuje, konfiguriše i implemetira u rad Službe za obezbeđenje svodi sistemsku grešku na minimum. Obrazloženje minimalne sistemske greške: Sistemi se postavljaju tako da se napajanja rade i tri nivoa (ups, agregat, mreža – redudantno), mrežna tehnologija koja se postavlja nema mogućnosti gubljenja prenosnog

signala zbog svoje topologije i tehnologije. Pouzdanost rada sistema i njihov integracije u studiji slučaja Kazneno popravnog zavoda u Pančevu gde je novinkorporirani sistem postaljen nije imao gubitaka i nepouzdanosti u radu od 2018 godine do danas, što ga čini maksimalno pouzdanim. Postojanje greške u ovakvom vidu sistema može biti prilikom implemetacije, obuke i postupanja čoveka u vanrednim događajima. Sofisticirani sistemi i način njihovog projektovanja zavisi od potrebe korisnika pa se sistem prema tome projektuje,konfiguriše i implementira. Primena ovakvih model integracije moguć je na svim tipovima objekata specijalne namene, sudovima, zdravstvenim i prosvetnim ustanovama itd.

VIII. Principi alarmiranja u studiji slučaja masovne tuče zatvorenika sa barikadiranjem

Mesto događaja: Blok na kome su smeštena 40 osuđena lica, jer do masovnih tuča može doći samo na mestima gde je skoncentrisan veći broj osuđenih lica. Aktivnost u trenutku masovne tuče i barikade: Slobodno vremenske aktivnost na bloku. OPIS DOGAĐAJA:

U 13:05 dolazi do vanrednog događaja masovne tuče osuđenih lica, dok se određeni broj osuđenika zabarikadirao u svojim sobama. Pripadnik Službe za obezbeđenje se u tom trnutku nalazi na svom radnom mestu sa koga putem sistema video nadzora prati aktivnost na bloku. Po izbijanju vanrednog događaja aktivira panik taster na sistemu za radio vezu i vrši blokiranje sektora STOP tasterom u svojoj nadležnoj zoni. Alarm koji je pripadnik Službe za obezbeđenje aktivirao automatizovano daje zvučnu signalizaciju i otvara zvučnik na radio uređaju koji u radijusu od 9 metara vrši direktan prenos zvuka pored autoamatizovanog prikaza zone u kojoj je nastao vanredni događaj na video zidu u Operativnom centru (snima u bazi podataka kao dikahni materijal). Dežurni zavoda po aktivaciji zvučnog signala prepoznaje vrstu vanrednog događaja (svai događa se definiše posebnom zvučnom signalizacijom).

Vreme za saznanja i preduzimanje mera je odmah po zvučnoj i vizualnoj signalizaciji. Napomena: U primeni neitegrisanog modela tehničke zaštite vreme saznanja i preduzimanje mera se znatno razlikuje.Neintegrisani modeli zahtevaju neprekidno nadgledanje sistema video nadzora od strane pripadnika Službe za obezbeđenje Pravoremenu intervenciju operatera u vidu brzine predefeinisanja video nadzora na zonu vanrednog događaja po uslovom da pripadnik Službe za obezbeđenje u takvim okolnostima radio vezom jasno i pravoremeno javi gde i kakav vanredni događaj je nastao. Dežurni zavoda mora uskladiti postupanje i intervneciju pripadnika Službe za obezbeđenje jer kod javljanja vanrednog događaja radio vezom koja nije digitalna i nije pravilno kofigurisana svi korisnici sistema imaju mogućnost slušanja prenosa informacije. Dok je kod pravilno kofiguranih digitalnoh sistema on podeljen zonski u komunikacione grupe, tako da ova pojava nije moguća.

Prilikom vanrednog događaja masovne tuče menadžment preduzima sledeće radnje dezurni zavoda mora: Locirati mesto sukoba;Uočiti veličinu grupe, razlog sukoba, sredstva napada;Izvršiti procenu nastale situacije;Izvršiti procenu broja pripadnika službe za obezbeđenje koji su prisutni, s obzirom na nastalu situaciju;Proceniti potrebu za aktiviranjem interventne jedinice službe za obezbeđenje;Isplanirati upotrebu materijalno-tehničkih sredstava;Izvršiti procenu i isplanirati ukoliko se ukaže potreba za evakuacijom osuđenih lica;Poziva prema planu grupu za intervenciju ili prema proceni situacije celokupni sastav službeFormira od trenutno prisutnih pripadnika i pripadnika koji su se odazvali na poziv grupu za razbijanje postavljenih zapreka, prati situaciju do dolaska starešine, priprema ljudstvo i potrebna sredstva (alat) za intervenciju, pojačava spoljno obezbeđenje.

Prati situaciju u delovima zavoda u kojima nije narušen red i bezbednost, angažuje deo ljudstva na održavanju situacije i sprečavanju širenja nereda. Kontrolisati vanrednu situaciju sa raspoloživim ljudstvom; Obavestiti Upravnika, načelnika službe za obezbeđenje, nadležnog starešinu i sledite njihova uputstva. Izvršiti razbijanje sukobljenih grupa, energičnom intervencijom, uz upotrebu sredstava prinude; Uspostavite red i mir, što je pre moguće; izvršiti zbrinjavanje povređenih lica; Proceniti potrebu za pozivanjem hitne pomoći, policijske uprave, vatrogasne-spasilačke jedinice; Identifikovati lica lišena slobode, učesnike sukoba (putem sistema za video obezbeđenje). Izvršiti pretres lica lišenih slobode, sa oduzimanjem nedozvoljenih predmeta i stvari; Uzeti izjave od lica lišenih slobode, izvršiti vezivanje učesnika sukoba; Izdvojiti lica lišena slobode, učesnike sukoba u posebne prostorije, do odluke Upravnika; Obezbediti mesto događaja i učesnike u sukobu. Uzeti pisane izveštaje od pripadnika službe za obezbeđenje o upotrebi mera prinude i sačiniti izveštaj o upotrebi mera prinude.

STAREŠINA: Vrši procenu situacije (broj i strukturu zabarikadiranih lica, mesto gde su se lica zabarikadirala, mogućnost prilaza i upotrebe šmrkova sa vodom i hemijskih sredstava, situaciju u delu zavoda i moguće prenošenje nemira, mogućnost radikalizacije situacije uzimanjem talaca). Vrši procenu sopstvenih snaga i sredstava: formira grupe za razbijanje barikade, savladavanje, vezivanje, izvođenje lica,za podršku (rezervu), za upotrebu hem. sredstava, pružanje prve pomoći.

IX. Zaključak

Osnovni pristup u projektovanju sistema tehničke zaštite treba da odgovara prirodi problema, što sa sobom nosi njihovu višeslojnost i skalabilnost, odnosno otvorenost projektovanih sistema za eventualnu buduću nadogradnju kako na nivo jednog sistema (npr. CCTV), tako i na nivou integralnog tehničkog rešenja. Projektovanje i instalacija sistema tehničke zaštite na nekom objektu je samo početak prihvatanja sistema kao efikasnog sredstva za zaštitu lica i materijalnih dobara u njemu. Sastavni deo projektnih zadataka je analiza bezbednosnih problema koja treba da posluži kao osnova za upoznavanje sa njihovim pojavnim oblicima, a u cilju pronalaženja odgovarajućih tehničkih i bezbednosnih rešenja. Služba za obezbeđenje, bez obzira na organizacioni oblik kojim se ostvaruje, predstavlja organizacionu celinu internih subjekata obezbeđenja u užem smislu, i u svom radu neretko se susreće sa izazovima i poslovima koje ne može samostalno da realizuje, već se oslanja na asistenciju drugih organa. Na

osnovu do sada izloženog može se zaključiti da sistem tehničke zaštite ustanova za izvršenje krivičnih sankcija čini zaokruženi sistem različitih mera, radnji i postupaka kojima se sistem drži na optimalnom nivou, sa ciljem predupređenja bezbednosnih rizika, po ustanovu, zaposlene i štićenike. Imajući u vidu navedeno može se zaključiti da optimalna i integralna tehnička zaštita ustanova za izvršenje krivičnih sankcija treba da obuhvati primenu sledećih sistema, i to: Video nadzor, Perimetrska zaštita, Protivprovalna zaštita, Kontrola obilaska objekta, Kontradiverziona zaštita, Kontrola pristupa i evidencija radnog vremena, Interfonski i videointerfonski sistemi, Sistem ozvučavanja, Sistem čuvanja i kontrole (evidencije) korišćenja ključeva, Mehanička zaštita, Sistem radio veza, Lični alarmni sistemi, Sistem osvetljenja perimetarskog kruga i svih prostora ustanove, Sistem bezprekidnog napajanja, Informacioni sistem i računarska mreža, Protivpožarni sistem, Elektromagnetna kompatibilnost sistema tehničke zaštite.

LITERATURA

[1] Ž. Nikač, R. Radovanović, and V. Zorić, "Privatna bezbednost u Srbiji – pravni osnovi i edukacija pripadnika," Teme: časopis za društvene nauke, vol. XIII, no. 1, pp. 203–223, Jan.–Mar. 2018.

[2] S. Stojanović, Skupštinska kontrola i nadzor sektora bezbednosti Srbije - priručnik. Beograd: OEBS, 2012, pp. 112–114.

[3] UNODC, Program obuke o ženama i zatvoru. Vienna: United Nations Office on Drugs and Crime, 2015, p. 16.

[4] Council of Europe, Priručnik za obuku o dodatnim sposobnostima zatvorskih službenika sa operativnim procedurama. Strasbourg: Council of Europe, pp. 45–46.

[5] N. Macanović, Funkcionisanje zatvora i resocijalizacija osuđenih lica. Banja Luka: Naučni rad, 2012.

[6] Z. Milanović and R. Radovanović, "Digital forensics in the context of information system protection," Bezbednost, vol. 55, no. 1, pp. 61–83, 2013.

[7] Đ. Ignjatović, Kriminologija. Beograd: Pravni fakultet Univerziteta u Beogradu, 2008, p. 178.

[8] J. Špadijer-Džinić, Zatvoreničko društvo. Beograd: Institut za kriminološka i sociološka istraživanja, 1973, pp. 62–63.

[9] L. M. Maruschak, HIV in Prisons 2001–2010. Washington, D.C.: U.S. Dept. of Justice, Bureau of Justice Statistics, 2012.

[10] Institut za mentalno zdravlje, Interni dokument, Beograd, 2005.

[11] I. Lazarević and R. Radovanović, Terorizam oružjem za masovno uništavanje. Beograd: Kriminalističko-policijska akademija, 2015.

[12] Pravilnik o načinu obavljanja poslova u službi za obezbeđenje u zavodima za izvršenje krivičnih sankcija, "Službeni glasnik RS," br. 21, Mar. 4, 2016; br. 104, Dec. 23, 2016.

[13] Z. Keković, S. Savić, N. Komazec, M. Milošević, and D. Jovanović, Procena rizika u zaštiti lica, imovine i poslovanja. Beograd: Centar za analizu rizika i upravljanje krizama, 2011.

[14] Z. Milanović and R. Radovanović, "Standard ISO/IEC 27005:2008 – osnov za menadžment rizika u sferi informacione bezbednosti," in Suprotstavljanje organizovanom kriminalu – pravni okvir, međunarodni standardi i procedure, Tara, Serbia, 2013, pp. 243–262.

[15] R. Simić and M. Bošković, Fizičko-tehnička zaštita objekata. Beograd: Institut bezbednosti, 1991.

[16] K. Đujić, Sistemi tehničke zaštite u ustanovama za izvršenje krivičnih sankcija. Beograd: Kriminalističko-policijska akademija, 2018.

[17] Microsegur, "Types of perimeter security systems," [Online]. Available: https://microsegur.com/en/types-of-perimeter-security-systems/

[18] Senstar, "Senstar LM100 Fence Sensor," [Online]. Available: https://senstar.com/products/fence-sensors/senstar-lm100/

[19] M. D. Dabhi, Geofencing: A Generic Approach to Real Time Location Based Tracking System. [Monograph].

[20] B. Ballad, T. Ballad, and E. Banks, Access Control, Authentication, and Public Key Infrastructure, Sep. 2010. [Online]. Available: https://books.google.ru/books?id=YIOAuSW0GAcC

[21] S. Harris, CISSP All-in-One Exam Guide. New York, NY, USA: McGraw-Hill, 2016, pp. 427–446.

Internet of Intelligent Technical Security Devices in Correctional Facilities Supporting the Decision-Making Process in Security Incident Situations

Kristijan Đujić
Juvenile Correctional Facility
Valjevo, Serbia
kristijan.djujic@gmail.com and ORCID 0009-0005-1846-3390

Martin Matijašević
Faculty of Business and Law
MB University
Belgrade, Serbia
martin.matijasevic@yahoo.com and ORCID 0009-0006-5840-7446

Radovan Radovanović
University of Criminal Investigation and PS
Belgrade, Serbia
radovan.radovanovic@gmail.com and ORCID 0000-0001-7302-8328

Saša Milić
Nikola Tesla Electrical Engineering Institute, Faculty of D and S
Belgrade, Serbia
sasa.milic@yahoo.com and ORCID 0000-0001-5757-3430

***Abstract*—This paper analyzes the Internet of intelligent technical security devices in correctional institutions as support for the decision-making process during security incident situations. By their function, correctional institutions are high-risk environments for security incidents. Intelligent technical security devices are structured into video surveillance and perimeter protection systems, communication maintenance devices, metal detection and recognition devices, access control and identification systems, fire detection systems, and mechanical protection systems. Through their integration, the technical security system becomes a functional whole. The integration of these systems should support the strategic and top levels of security management in the decision-making process during security incident situations.**

***Keywords*—facilities, technical, security, intelligent, system, incidents**