Analiza i koncept zaštite financijske institucije

Poljak, Lovro

VELEUČILIŠTE U KARLOVCU
Specijalistički diplomski stručni studij
Sigurnost i zaštita

LOVRO POLJAK

ANALIZA I KONCEPT ZAŠTITE FINANCIJSKE INSTITUCIJE

ZAVRŠNI RAD

KARLOVAC, 2015.

VELEUČILIŠTE U KARLOVCU
SPECIJALISTIČKI DIPLOMSKI STRUČNI STUDIJ
SIGURNOST I ZAŠTITA

Usmjerenje: Sigurnost i zaštita

Karlovac, 2015.04.10.

ZADATAK ZAVRŠNOG RADA

Student: LOVRO POLJAK Matični broj: 0420411027

Naslov: ANALIZA I KONCEPT ZAŠTITE FINANCIJSKE INSTITUCIJE

Opis zadatka:

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

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
2015.04.10.	2015.06.29.	2015.07.09.

Mentor:
dr. sc. Vladimir Tudić, viši pred.

Predsjednik Ispitnog povjerenstva:
dr. sc. Nikola Trbojević, prof. visoke škole

PREDGOVOR

Izjava

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

Zahvala

Zahvaljujem se mojoj životnoj partnerici, Adriani Glažar, prijatelju Goranu Vidakoviću na nesebičnoj pomoći i strpljenu u stjecanju znanja o tehničkoj zaštiti, mentoru dr. sc. Vladimiru Tudiću na savjetima, konzultacijama i pomoći pri izradi ovog završnog rada. Hvala svima koji su mi bili podrška kroz moj studij, a posebno mojoj obitelji.

SAŽETAK

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

Kako se cjelokupno poslovanje jedne tvrtke vodi ekonomskom logikom tako će i u slučaju određivanja oblika, razine i načina upravljanja sigurnošću prevladati ekonomska logika. Prema tome potrebno je elaborirati sve moguće ugroze koje dovode do destrukcije i pronaći oblike i odrediti razinu zaštite koja će spriječiti ili umanjiti učinke ugrožavanja. Normativni i pragmatični pristup kojim se udovoljava samo zakonu, bez traženja funkcije u djelatnosti ili se kopiraju rješenja drugih zadovoljavajući samo formu nespojivo je sa suvremenim upravljanjem sigurnošću.

Da bi se odredilo optimalno rješenje potrebno je identificirati opasnosti, odrediti posljedice ugrožavanja, odrediti rizik i predložiti tehničko rješenje i mjeru tjelesne zaštite u svrhu smanjenja rizika na prihvatljivu razinu.

Tehnička zaštita predstavlja skup radnji kojima se neposredno ili posredno zaštićuju ljudi i njihova imovina, a provodi se tehničkim sredstvima i napravama te sustavima tehničke zaštite kojima je osnovna namjena sprječavanje protupravnih radnji usmjerenih prema štićenim osobama ili imovini. Sredstvima i napravama tehničke zaštite, podrazumijevaju se sredstva i naprave za tjelesno sprječavanje nedopuštenog ulaska osoba u štićeni objekt, a pored raznih mehaničkih koriste se i elektronički sigurnosni sustavi koji omogućuju učinkovitu zaštitu štićenog objekta. Ovo su definicije iz Pravilnika o uvjetima i načinu provedbe sustava tehničke zaštite, prema kojima se isti dijele na protuprovalni sustav, protuprepadni sustav, vatrodojavni sustav, sustav kontrole prolaza, sustav video nadzora, sustav mehaničke zaštite.

Ključne riječi: Prosudba ugroženosti, tehnička zaštita, koncept zaštite, sustav zaštite, upravljanje sigurnošću

SUMMARY

The protection concept enables effective risks reduction arising from safety factors. Protection concept determines actions, procedures and responsibilities of individual subjects in a wide range of security tasks such as vulnerability assessment, technical protection, physical protection, fire protection, delivery of money, control of contractors, system design, operation control center, system protection management. As the entire business of a company leads to economic logic so it is the same in the case of determining the forms, levels and modes of safety management. Therefore it is necessary to elaborate on any possible threat that lead to destruction and to find forms and determine the level of protection that will prevent or reduce the effects of threat. The normative and pragmatic approach that complies with only the law, without seeking activities in business, or functions that are copied from other solutions with only function to comply with the standard is incompatible with modern safety management. In order to determine the optimal solution it is necessary to identify the hazards, determine the consequences of threats, assess the risk and propose a technical solution and the measure of physical protection to reduce the risk to an acceptable level.

Technical security represents a set of actions that directly or indirectly protect people and their property, and is carried out technical resources and devices and security systems where the primary purpose is prevention of illegal acts directed against protected persons or property. Technical security devices, imply equipment for the physically prevention of unauthorized entry of a person into the protected facility, Besides a variety of mechanical security systems there are an electronic security systems that provide effective protection.

All this above are defined in the Ordinance concerning the conditions and manner of implementation of technical protection, by which are shared in the burglar alarm system, CCTV video surveillance system, fire alarm system, access control, video surveillance system, system of mechanical protection.

Key words: vulnerability assessment , technical protection, the concept of protection, system protection, security management.

SADRŽAJ

POPIS SLIKA I TABLICA

1.KONCEPT ZAVRŠNOG RADA

1.1. Uvod u predmetno područje

Financijske institucije zbog svoje prirode poslovanja oduvijek su bile najugroženije od raznih mogućih ugroza pa se prema njima treba odnositi vrlo temeljito, sagledavajući sve čimbenike koji utječu na sigurnost bilo poslovanja, klijenata, zaposlenika ili okoline. Kada kažemo ugroza ovdje se misli na čitav niz kaznenih djela kao i na ugrožavanje života i zdravlja ljudi u okolini. Analizirajući razne oblike kriminaliteta (teške krađe, krađe, provalne krađe, razbojništva i razbojničke krađe) u odnosu na tip novčarske institucije uočava se neprekidan rast broja zabilježenih slučajeva. U strukturi kaznenih djela najzastupljenija su razbojništva. Iz podataka za izvršena razbojništva (tablica 1) i prouzročenu materijalna štetu (tablica 2) za kaznena djela razbojništva u Republici Hrvatskoj u razdoblju od 5 godina uključujući 2012. vidljivo je da banke uz trgovine i mjenjačnice prednjače u financijskoj šteti koja je učinjena prilikom razbojništava bez obzira što je broj samih kaznenih djela najmanji.

Tablica 1: razbojništva

Razbojništva	2008	2009	2010	2011	2012
Pošte	41	25	34	39	47
Banke	10	8	9	37	23
Mjenjačnice	9	33	19	27	15
Kuće i stanove	35	37	42	46	77
Trgovine	211	289	257	323	318
Benzinske crpke	69	101	91	79	90
Kioske	81	93	118	102	106
Stambene zgrade	23	17	19	17	25
Otvoreni prostor	267	240	197	217	246
Kladionice*	213	262	221	272	420
Ostalo	213	262	221	272	420
UKUPNO	**959**	**1367**	**1228**	**1431**	**1787**

Također ne smijemo zaboraviti reputacijsku štetu nastalu prilikom ovakvih događaja koji je gotovo nemoguće izmjeriti.

Tablica 2: Materijalna šteta za kaznena djela razbojništva u kunama

Razbojništva	2008	2009	2010	2011	2012
Pošte	16.146.836	490.253	726.579	1.567.989	693.050
Banke	1.974.790	842.525	2.797.099	4.659.766	2.086.977
Mjenjačnice	202.920	2.749.849	1.039.500	1.664.400	2.036.574
Kuće i stanove	1.054.337	1.083.860	251.524	352.578	1.200.025
Trgovine	1.545.822	1.266.415	4.957.663	4.335.722	2.866.591
Benzinske crpke	1.736.369	1.980.630	908.708	921.898	923.802
Kioske	168.993	210.301	156.161	479.930	204.773
Stambene zgrade	278.284	85.626	278.750	63.160	73.150
Otvoreni prostor	4.060.746	3.035.057	583.053	1.198.377	2.678.278
Kladionice	1.422.584	1.309.516	778.046	996.017	635.203
Ostalo	2.634.528	6.061.417	¸2.608.174	7.893.563	7.418.379
UKUPNO	**31.226.209**	**19.115.449**	**12.477.083**	**24.133.400**	**20.816.802**

Najčešće se svi dokumenti vezani za zaštitu i sigurnost klasificiraju kao vrlo tajni, tajni ili barem kao poslovna tajna tako da neki od bitnijih i specifičnih podataka za analiziranu instituciju neće moći biti prikazani zbog zaštite tajnosti podataka. Svi elementi analize biti će što je više moguće poopćeni i neće se odnositi samo na reprezentativnu financijsku instituciju nego općenito za sve.

1.2. Opis problema

Obzirom na trendove sve veću upotrebu tehničke zaštite pri osiguravanju financijskih institucija javlja se potreba za konceptualnim rješenjima koja objedinjuju sve sustave zaštite. Ista su individualna za pojedinog investitora i u skladu sa zahtjevima i financijskim planovima organizacije. Stručnjaci za sigurnost mnogo će lakše pratiti i po potrebi nadopunjavati zaštitu svoje institucije ako oblikuju koncept zaštite kao formalni akt koji će sagledati sve navedene ugroze kao i načine kako ih što efikasnije spriječiti. Koncept mora biti tako konstruiran da nametne standard pri samom projektiranju, izvođenju i nadzoru te kasnijoj reviziji i održavanju svih segmenata zaštite.

Ovaj akt mora se temeljiti na slijedećem:

- trenutno važećoj zakonskoj regulativi za predmetno područje
- trenutno važećim zahtjevima osiguravajućih kuća
- razini kriminaliteta u državi
- pratećem tehnološkom nivou
- radnim procesima u instituciji
- empirijskim saznanjima o štetnim događajima unutar institucije

Osim nametanja standarda koncept mora osigurati usklađenost sa važećom zakonskom regulativom i biti ažuran u svakom trenutku sa svim promjenama u procesima financijske institucije kao i sa promjenama zakonske regulative.
Kako smo svjedoci svakodnevnog razvoja tržišta i konkurentnosti raznih izvođača i opreme na tržištu koncept osim navedenog mora osigurati brzu i laku promjenu strateškog partnera ugovorenog za poslove tehničke zaštite kako bi kontinuirano

osigurali kvalitetu zahtijevanu od investitora. Kako je bitan formalni koncept zaštite tako i njegova pravovremena revizija ili analiza na osnovu koje se on može uvijek ažurirati sa najnovijom regulativom a također i sa primjenom najnovijih tehnologija. Ovim radom dan je primjer zaštite financijske institucije i to kroz izradu prosudbe ugroženosti i procesa analize koji kreće od komentara zakonske regulative pa preko pregleda postojećih sustava, a završava sa završnom ocjenom stanja sigurnosti i prijedlogom budućih mjera za poboljšanje sigurnosti te na kraju zaključak. Potrebno je odmah naglasiti da je vrlo bitan element u planiranju zaštite kroz koncept i osiguranje sredstava za implementiranje svih sustava što također treba na vrijeme planirati i rezervirati. Često se menadžer sigurnosti unutar organizacije bavi i sa financijskim aspektom zaštite zbog ograničenih sredstava uz koja mora zadovoljiti stavljene zahtjeve za sigurnošću. Zato je bitno da on bude što je više pozicioniran u strukturi tvrtke i odgovoran samo upravi.

1.3. Cilj i zadaci Završnog rada

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

1.4. Metode korištene za izradu Završnog rada

Za izradu Završnog rada korištena je uglavnom deskriptivna metoda (metoda zapažanja i opisivanja fenomena), uključujući studij dokumentacije, sistemsko promatranje, i trenutačno zapažanje. Studij dokumentacije podrazumijeva prikupljanje, analizu i obradu podataka. Podaci su prikupljeni temeljitim pregledom i analizom raspoložive dokumentacije, kao i obilaskom objekta. Predmet istraživanja je analiza sustava tehničke zaštite, odnosno provjera koncepta zaštite (ako isti uopće postoji) od strane neovisne stručne osobe. U istraživanju se pošlo od toga što je prosudba ugroženosti, koji je koncept zaštite, kako je on formiran, na koji način je implementiran u praksi, te koji su propusti i moguće nadogradnje istog da se osigura optimalan nivo zaštite u skladu sa zakonskim okvirima.

Obrađujući temu korišteni su:

- Zakonski propisi i norme koje se odnose na sustave tehničke zaštite
- Literatura koja obrađuje problematiku sustava tehničke zaštite.
- Dostupna projektna dokumentacija sa nekih od objekata
- Obilazak objekata i trenutačno zapažanje
- Pohađanje stručnih seminara

2. PRIKAZ REZULTATA RADA

2.1. Propisi za sustave tehničke zaštite

Pregledom propisa koji pravno reguliraju ovo područje pronađen je veliki broj pravnih akata i normi, a ovo su oni najvažniji među njima:

• Zakon o privatnoj zaštiti (NN 68/03., 31/10., 139/10.)

• Zakon o minimalnim mjerama zaštite u poslovanju gotovim novcem i vrijednostima (NN 173/03., 150/05.)

• Kazneni zakon (NN 125/11.)

• Zakon o tajnosti podataka (NN 79/07., 86/12.)

• Zakon o igrama na sreću (NN 87/09.)

• Zakon o informacijskoj sigurnosti (NN 79/07.)

• Zakon o sprječavanju nereda na športskim natjecanjima (NN 117/03., 71/06., 43/09., 34/11.)

• Zakon o kritičnim infrastrukturama (NN 56/13.)

Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN 198/03.)

• Pravilnik o prostornim i tehničkim uvjetima za priređivanje igara na sreću u kasinima, na automatima i uplatnim mjestima kladionica (NN 38/10., 130/10., 69/11., 15/12.)

• Pravilnik o načinu i uvjetima obavljanja poslova privatne zaštite na javnim površinama (NN 36/12).

Jedan od najvažnijih zakona koji se odnosi na financijske institucije je Zakon o minimalnim mjerama zaštite u poslovanju gotovim novcem i vrijednostima (NN, 173/03. i 150/05.). U njemu su dani temeljni uvjeti na koji način svrstati institucije i na koji način ih optimalno zaštititi, pa se tako sukladno ovom zakonu financijske institucije svrstavaju u 3 slijedeće kategorije:

I. kategorija – Hrvatska narodna banka, poslovnice FINA-e, banke, stambene štedionice, poštanski uredi Hrvatskih pošta
- poslovnice ove kategorije moraju se štititi sa protuprovalnim i protuprepadnim sustavom sa centraliziranom dojavom i nadzorom alarma, neprekidnim video nadzorom s mogućnošću pohranjivanja video zapisa, te tjelesnom zaštitom.

II. kategorija – mjenjačnice, poslovnice Hrvatske lutrije, kladionice, štedno-kreditne zadruge
- poslovnice ove kategorije moraju se štititi sa protuprovalnim i protuprepadnim sustavom sa centraliziranom dojavom i nadzorom alarma ili neprekidnim video nadzorom sa mogućnošću pohranjivanja video zapisa, te tjelesnom zaštitom.

III. kategorija – bankomati
- poslovnice ove kategorije moraju instalirati neprekidni nadzor komunikacijske veze bankomata s dojavnim centrom, te alarm otvorenih vrata trezorskog dijela bankomata.
Osim navedenih mjera dodatno treba zaštititi zajedničkom primjenom tjelesne zaštite i sustava tehničke zaštite centralne trezore financijske institucije. Prijevoz

gotovog novca također je reguliran ovim zakonom i obveza je institucije provoditi sve navedene mjere zaštite koje nisu predmet ove analize.

Iznimka koja je moguća sukladno izmjenama i dopunama ovog Zakona je da novčarske institucije, njihove poslovne jedinice i poslovna mjesta I. i II. kategorije u kojima je zaposleno do pet zaposlenika koji neposredno rukuju gotovim novcem ili vrijednostima ne moraju ispunjavati uvjet da imaju tjelesnu zaštitu ako izvedu pregradnju radnog prostora zaposlenika neprobojnim pregradama u visini etaže i protuprovalna vrata od prostora koji su dostupni strankama i drugim osobama. Zakonom je također utvrđeno da se sve sigurnosne mjere mogu regulirati ako se prosudbom ugroženosti utvrdi da je ugroženost smanjena a MUP da suglasnost na tu prosudbu (Prilog 1).

Osim ovog zakona po zakonu o privatnoj zaštiti obveza je svih vlasnika sustava izraditi prosudbu ugroženosti i sigurnosni elaborat u kojem se također objekt mora svrstati u neku od kategorija ugroženosti. Postoji 6 kategorija ugroženosti objekta a za svaku su propisane obavezne mjere zaštite:

I. kategorija - NAJVIŠI STUPANJ ZAŠTITE koji predviđa:

- mehaničku i tehničku zaštitu kojom se signalizira neovlašten ulazak u štićeni prostor i dojavljuje na CDS (Centralno dojavni sustav),
- tehničku zaštitu kojom se prati kretanje u štićenom prostoru i pojedinačno štićenim prostorijama (kontrola prolaza i video nadzor) uz video zapis,
- zaštitu pojedinačnih vrijednosti pomoću specijalnih kasa, trezora i sl.,
- integralnu zaštitu s najmanje jednim (1) lokalnim nadzornim mjestom i sustavom veze sa zaštitarima na štićenom objektu,
- sigurnosni Plan postupanja i procedure u slučajevima pretpostavljenih incidentnih situacija.

II. kategorija - VISOKI STUPANJ ZAŠTITE koji predviđa:

- mehaničku i tehničku zaštitu kojom se signalizira neovlašten ulazak u štićeni prostor i dojavljuje na CDS,

- tehničku zaštitu kojom se prati kretanje u štićenom prostoru (kontrola prolaza i video nadzor) uz video zapis,
- integralnu zaštitu s najmanje jednim (1) lokalnim nadzornim mjestom i sustavom veze sa CDS-om.

III. kategorija - VIŠI STUPANJ ZAŠTITE koji predviđa:

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

IV. kategorija - SREDNJI STUPANJ ZAŠTITE koji predviđa:

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

V. kategorija - NIŽI STUPANJ ZAŠTITE koji predviđa:

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

VI. kategorija - MINIMUM ZAŠTITE koji predviđa:

- mehaničku zaštitu bez uporabe elektroničkih naprava,
- obične cilindarske brave,
- obične ograde bez tehničkih elemenata (osim za stanove).

Za izradu prosudbe ugroženosti i sigurnosnog elaborata dana je preporuka CEHA zaštitara koja predlaže sistematiku kategorizacije objekta i čimbenike koji na istu utječu pa projektanti najčešće koriste ovu publikaciju prilikom izrade prosudbe ugroženosti iako ona nije propisana Zakonom.

Osim poštivanja zakonskih propisa, sustav i oprema moraju zadovoljiti zahtjeve iz slijedećih normi:

- HRN EN 50130-4:1997 Alarmni sustavi - 4.dio:Elektromagnetska kompatibilnost, zahtjevi na otpornost za dijelove vatrodojavnih protuprovalnih i socijalnih alarmnih sustava

- HRN EN 50130-4/A1:2000 Elektromagnetska kompatibilnost -- Norma za porodicu proizvoda: Zahtjevi za otpornost na smetnje za dijelove vatrodojavnih, protuprovalnih i socijalnih alarmnih sustava

- HRN EN 50130–5:2000 Alarmni sustavi - 5.dio: Metode ispitivanja pri utjecaju okoliša

- HRN EN 50131-1:2000 Alarmni sustavi - Protuprovalni sustavi- 1.dio:Opći zahtjevi

- HRN EN 50131-5:2008 Alarmni sustavi -- Protuprovalni i protuprepadni sustavi -- Dio 2-4: Zahtjevi za kombinirane pasivne infracrvene i mikrovalne detektore (EN 50131-2-4:2008)HRN EN 50130-4/A1:2000 Elektromagnetska kompatibilnost -- Norma za porodicu proizvoda: Zahtjevi za otpornost na smetnje za dijelove vatrodojavnih, protuprovalnih i socijalnih alarmnih sustava

- HRN EN 50132-5-1:2012 Alarmni sustavi -- Sustavi nadzora pomoću TV zatvorenog kruga za uporabu u primjenama zaštite -- Dio 5-1: Video prijenos -- Opći zahtjevi za karakteristike video prijenosa (EN 50132-5-1:2011+AC:2012)HRN EN 50132-4-1:2004 Alarmni sustavi -- Sustavi nadzora pomoću TV zatvorenog kruga za uporabu u primjenama zaštite -- Dio 4-1

- HRN EN 50132-5:2004 Alarmni sustavi -- Sustavi nadzora pomoću TV zatvorenog kruga za uporabu u primjenama zaštite -- 5. dio: Video prijenos

- HRN EN 50132-7:2013 Alarmni sustavi -- Sustavi nadzora s pomoću TV zatvorenog kruga -- 7. dio: Upute za primjenu

- HRN EN 50136-1-/A1:2004 Alarmni sustavi -- Sustavi i uređaji za prijenos signala alarma -- Dio 1-: Opći zahtjevi za sustave za prijenos signala alarma

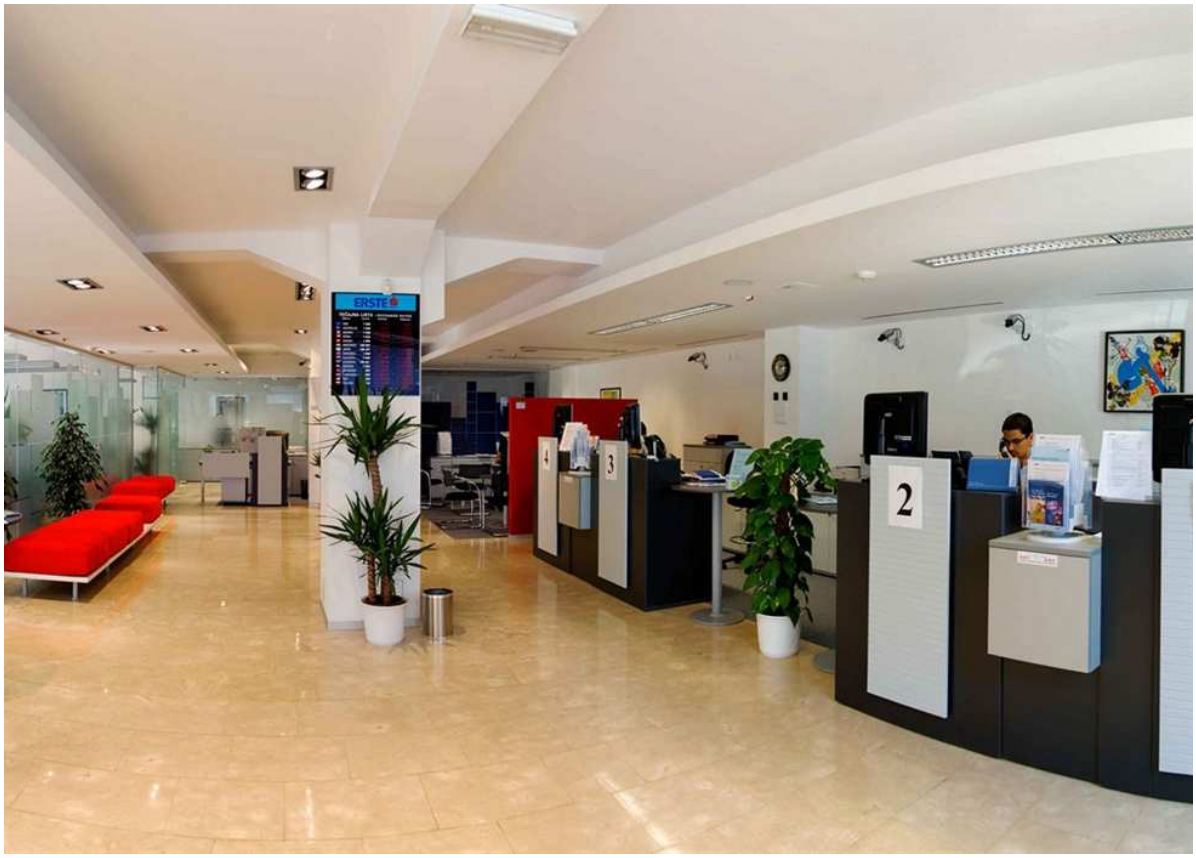
- HRN EN 50136-1-:2000 Alarmni sustavi -- Sustavi i uređaji za prijenos signala alarma -- Dio 1-: Opći zahtjevi za sustave za prijenos signala alarma

- HRN EN 50136-1-2:2000 Alarmni sustavi -- Sustavi i uređaji za prijenos signala alarma -- Dio 1-2: Zahtjevi za sustave koji primjenjuju prijenosne putove namijenjene za signale alarma

- HRN EN 50136-1-3:2000 Alarmni sustavi -- Sustavi i uređaji za prijenos alarma -- Dio 1-3: Zahtjevi za sustave s digitalnim komunikatorima koji primjenjuju javnu komutiranu telefonsku mrežu

2.2. Opis financijske institucije i procesa unutar iste

Predmetna financijska institucija koja je analizirana u ovom radu posluje sa građanima i tvrtkama kroz nekoliko tipova poslovnica.
Postoje klasične **gotovinske poslovnice** (slika 1) za rad s klijentima preko šaltera s nekoliko odvojenih otvorenih radnih mjesta za osobne bankare na kojima se ne barata s gotovinom.



Slika 1. Predodžba izgleda tipične bankovne gotovinske poslovnice

Jedna prostorija višeg stupnja zaštite projektirana je za smještaj kase te je izvedena u skladu sa sigurnosnim zahtjevima. Procedurama je definiran put kojim se dostavlja novac do blagajni ili trezora s vremenskim zatezanjem otvaranja na šalterima kao i dotacija i odvoz viška novca izvana. Ovi kritični putovi moraju biti posebno štićeni kontrolom prolaza i sustavom video nadzora. Poslovnice su uglavnom štićene i tjelesnom zaštitom osim nekih koje imaju implementirane sigurnije sustave zaštite

kao što su cijevna pošta ili interlocking vrata na ulazu i sl., pa je MUP dao suglasnost da se oslobode tjelesne zaštite. Zaštitar je prisutan prilikom dotacije

Slika 2: Predodžba trezora građana

novca, punjenja bankomata ili podizanja veće količine gotovog novca pa su ovi procesi uz njegovu prisutnost mnogo sigurniji.

U nekoliko poslovnica ovog tipa postoje i trezori građana (Slika 2) u koje klijenti pohranjuju svoje vrijednosti, oni su zaštićeni slično kao i prostorije sa kasom u poslovnici.

Slika 3: Predodžba 24 satne zone

Osim ovakvih poslovnica postoje i **24 satne zone** (slika 3) u kojima se nalaze samouslužni uređaji bez djelatnika banke. Pod samouslužnim uređajima misli se na uplatno-isplatne bankomate, dnevno-noćne trezore, aparate za virmanske uplate, i aparate za brojanje kovanica. U ovakvim poslovnicama konceptom su predviđene drugačije mjere zaštite jer protuprovalna zaštita mora biti aktivna 24 sata a protuprepadna nije uopće potrebna osim u trenucima punjenja samouslužnih uređaja sa gotovinom.

U 24 satnu poslovnicu ući mogu samo korisnici kartica kojima mogu izvršiti transakciju. Oni se karticom autoriziraju na čitaču prilikom ulaza nakon čega se odobrava ulaz. Za poslovnice ovakvog tipa bitan je što kvalitetniji sustav video nadzora iz razloga što u poslovici nema osoblja i često je potreban uvid u snimljeni

materijal zbog reklamacija. Pod kvalitetnijim misli se na dovoljnu količinu kamera, po barem jedna za svaki uređaj i za sve procese punjenja i pražnjenja kao i što veći broj slika u sekundi po pojedinoj kameri. Poseban naglasak pri zaštiti poslovnica ovog tipa bio bi na samom procesu punjenja ili pražnjenja gotovine jer je to najkritičniji trenutak pa je analizirana institucija konceptom propisala blokiranje ulaznih vrata u trenutku otvaranja i skidanja zaštite na uređajima. Ovo je potrebno izvesti automatski da se izbjegne mogućnost sabotaže od strane osoblja.

Slika 4: Predodžba regionalnog trezora

Slijedeći tip objekata su regionalni trezori (Slika 4) u kojima se čuvaju velike količine gotovine iz kojih se dostavlja gotovina poslovnicama, pune bankomati i sl. Naravno da su ovi objekti posebno štićeni zbog količine novca koja se nalazi u njima pa se stoga i projektiraju po posebnim uputama. Njihovu zaštitu uvelike diktiraju i osiguravajuće kuće koje se zbog velikih iznosa osiguranih svota moraju dodatno reosigurati kod vanjskog reosiguravatelja. Zbog toga se u projektiranju traže visoki nivoi zaštite. U regionalnom trezorima posebna se pozornost posvećuje dovozu i odvozu gotovog novca jer ovdje se danonoćno izmjenjuju blindirana vozila raznih zaštitarskih tvrtki. Brojanje novca također je potrebno detaljnije snimiti zbog kasnijeg utvrđivanja odgovornosti u slučaju manjka ili viška novca.

Slika 5: Predodžba bankomata

Kao zadnji tip komunikacije sa klijentima su danas nezaobilazni **bankomati (Slika 5)** na izdvojenim lokacijama kojih ima praktički u svakom mjestu u Hrvatskoj. Njihova pozicija ovisi o broju klijenata banke na pojedinim područjima a uglavnom su to razne trgovine, knjižnice ili vanjski samostojeću uređaji. Bankomati su spojeni na svoju mrežu kojom se dojavljuju kvarovi, potrebe za punjenjem ili servisom, a pune ih ovlaštene zaštitarske tvrtke s kojima je sklopljen ugovor.

Ugrađuje se više vrsta bankomata kao što isplatni bankomati, isplatni bankomati s depozitom, uplatno/isplatni bankomati, samo uplatni banomati.

2.3. Analiza postojećih sustava zaštite u poslovnicama

2.3.1. Protuprovalni sustav

Protuprovalni sustav u svim poslovnicama baziran je na mikroprocesorskom centralnom uređaju (slika 6). Takav sustav proširiv je do 128 ulaznih zona detekcije, ima mogućnost telefonske dojave na nadzorni centar, a dodatno je proširiv s LAN i GSM komunikatorom.

Slika 6: Predodžba mikroprocesorskog centralnog uređaja

Centralni uređaj može se programski podijeliti na 8 nezavisnih sektora (particija), sa 16 mogućih mjesta upravljanja pomoću LCD tipkovnica (slika 7).

Slika 7: Predodžba LCD tipkovnice

Uređajem može upravljati do 1000 korisnika, pomoću svojih kodova koji mogu biti četveroznamenkasti ili šesteroznamenkasti. Zone detekcije na ovom centralnom uređaju mogu se izvesti kao nadzirane sa jednim ili dva otpornika ili kao nenadzirane, a svi kablovi do perifernih uređaja zaštićeni su 24 sata od sabotaže.
Osim navedenih proširenja moguće je dodati do 8 dodatnih napajanja od 2A za napajanje perifernih uređaja, 16 modula s tranzistorskim izlazima, i modulom za bežične detektore. Sustav štiti korisnika od provale van radnog vremena poslovnice osim u nekim posebnim particijama koje su štićene 24 sata npr. server soba, ili bankomat.

Slika 8: Predodžba dualnog detektora pokreta

Zaštita od provale osigurava se dualnim detektorima pokreta (slika 8) koji detektira pokretne objekte, a najviše se koristi za ljude. Detektor pokreta se često integrira kao dio sustava koji automatski izvršava neki zadatak ili upozorava korisnika na pokret u prostoru. Detektor pokreta je važna komponenta svakog sigurnosnog sustava, bilo da se radi o automatiziranoj kontroli rasvjete, kontroli doma, automatiziranom video nadzoru te drugim korisnim sustavima.

Detektor pokreta može služiti kao aktivator kamere za video nadzor. Kamere za video nadzor mogu biti kontrolirane automatski, pomoću detektora kretanja te mogu biti i sakrivene u samom detektoru.

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

Postoje i detektori koji se ne aktiviraju na manje objekte. Takvi detektori se koriste u prostorima gdje postoji mogućnost lažnog aktiviranja alarma od strane manjih životinja, kućnih ljubimaca, psa čuvara i slično.

Slika 9: Predodžba detektora loma stakla

Zaštita od provale osigurava se i detektorima loma stakla (Slika 9) s analizom zvuka koji reagira na specifične frekvencije zvuka loma stakla. Osjetljivost se podešava potenciometrom, a može se montirati na zid i strop. Maksimalna osjetljivost je 10 m x 10 m, a minimalna osjetljivost je 3 m x 3 m Obično imaju MOV zaštitu od statičkog pražnjenja, te su neosjetljivi na radio smetnje. Imaju LED za signalizaciju alarmnog stanja.

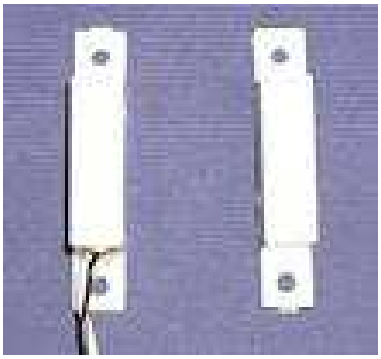
Slika 10: Predodžba detektora šuma

Zaštita od provale osigurava se i detektorima šuma (slika 10) koji omogućuju pokrivanje od 1m do 14 m s tri odvojena kanala za detekciju tipičnih frekvencija provale, uz istovremenu neosjetljivost na frekvencije iz okoline zbog čega osiguravaju pouzdan rad bez lažnih alarma. Imaju mogućnost podešavanja

osjetljivosti u 5 koraka po 6 dB, te uz to imaju LED za signalizaciju alarmnog stanja.

Obično se postavljaju na stijene bankomata, a prema procjeni ugroženosti i sigurnosnom elaboratu postavljaju se i na zidove, podove i stropove strateških prostorija štićenog objekta. Jedan od takvih primjera su centralni ili regionalni trezori. Detektroi šuma detektiraju vibracije bušilica, čekića, uređaja i strojeva za rezanje, varenje, nabijanje i slično. Primjenom bilo kojih od navedenih alata detektor aktivira alarm protuprovalne centrale.

Zaštita od provale osigurava se i magnetskim kontaktima (slika 11) na štićenim vratima.



Slika 11: Predodžba magnetskih kontakata

Dualni detektori koriste se zbog prevencije lažnih alarma jer koriste dvojnu (mikrovalnu i infracrvenu) tehnologiju za detekciju pa su imuni na lažne alarme od ostalih tipova detektora pokreta. Aktivacija alarma nakon prorade nekog od detektora manifestira se zvučnim i svjetlosnim uzbunjivanjem na samom objektu (najčešće jedna vanjska i barem jedna unutarnja sirena s bljeskalicom) te paralelno s odašiljanjem signala prema dojavnom centru putem telefonske linije, gsm komunikatora ili LAN veze. Ovaj signal može trenutno pozivati interventnu ekipu a potom po potrebi i policiju.

2.3.2. Protuprepadni sustav

Protuprepadni sustav kombinacija je tehničke, mehaničke i tjelesne zaštite. U osnovi gledano s tehničke strane on se sastoji od panik šine (slika 12) i panik tipke (slika 13) koje su spojene na centralni uređaj. U slučaju prepada, aktiviranjem tipkala ili šine prosljeđuje se tihi signal u dojavni centar koji odmah upućuje intervenciju.

Slika 12 : Predodžba panik šine

Slika 13: Predodžba panik tipke

Panik tipke mogu biti fiksirane na stol, ili kao bežični element dodijeljene korisniku. Osim samih tipkala za dojavu prepada koriste se i šifre prisile. Šifra prisile koristi se za isključenje alarma pod prisilom. U tom slučaju na dojavni centar također se prosljeđuje signal o prepadu dok na samom objektu nema nikakve indikacije o pokretanju dojave.

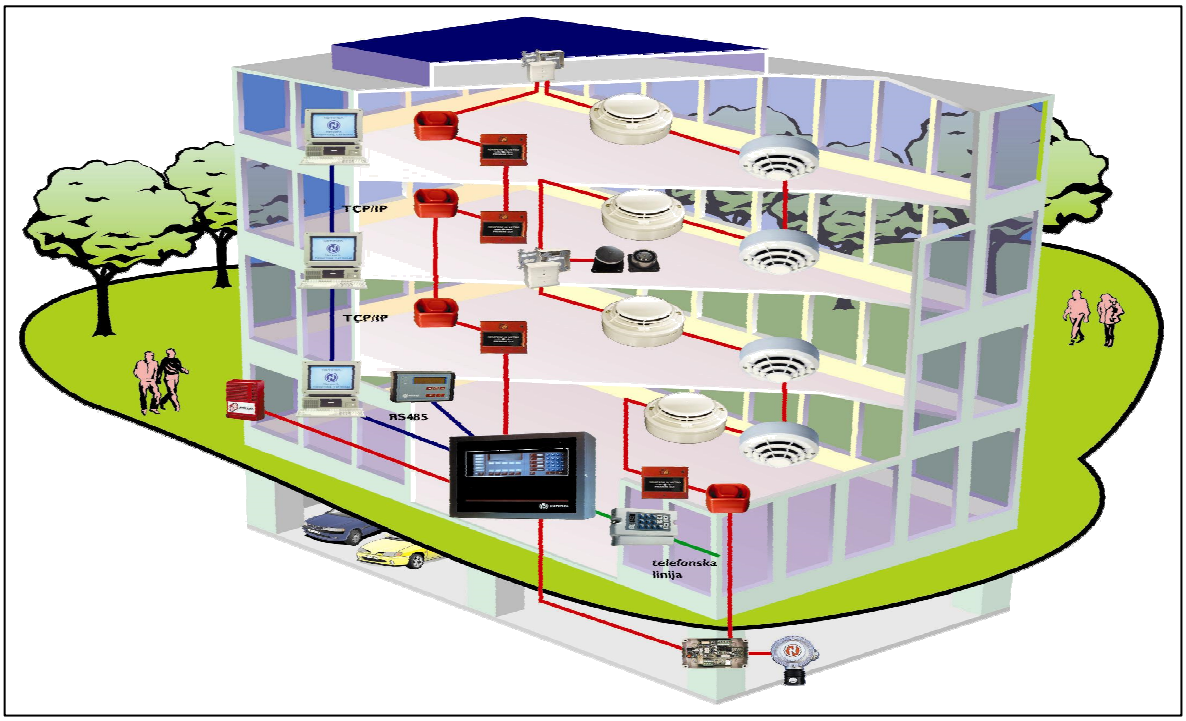
U posebnim situacijama za prevenciju prepada mogu se koristiti i posebni uvjeti na objektu koji kada se ispune moraju aktivirati dojavu. Jedan primjer je uvjet kada su

Slika 14 : Predodžba naljepnice

dvoja vrata u trezoru koja su u interlock izvedbi otvorena u isto vrijeme. Ovo stanje je nemoguće u normalnim uvjetima rada pa odmah indicira na mogućnost prepada i ako je tako projektom zadano upućuje dojavu na dojavni centar. Bitne stvari za prevenciju prepada su i kamere i informiranje korisnika naljepnicama (slika 14) postavljenim u poslovnici kao i razna vremenska zatezanja do pristupa gotovini. Vremenska zatezanja mogu se izvesti kao zadrška na kontroliranim vratima prema nekom važnijem dijelu objekta (vrata nije moguće otvoriti dok ne istekne određeni vremenski period), ili kao vremensko zatezanje na time-trezoru u kojem se čuva gotovina na šalterskom radnom mjestu. Također zadrška može biti izvedena na samoj kasi u kojoj se čuva gotovina.

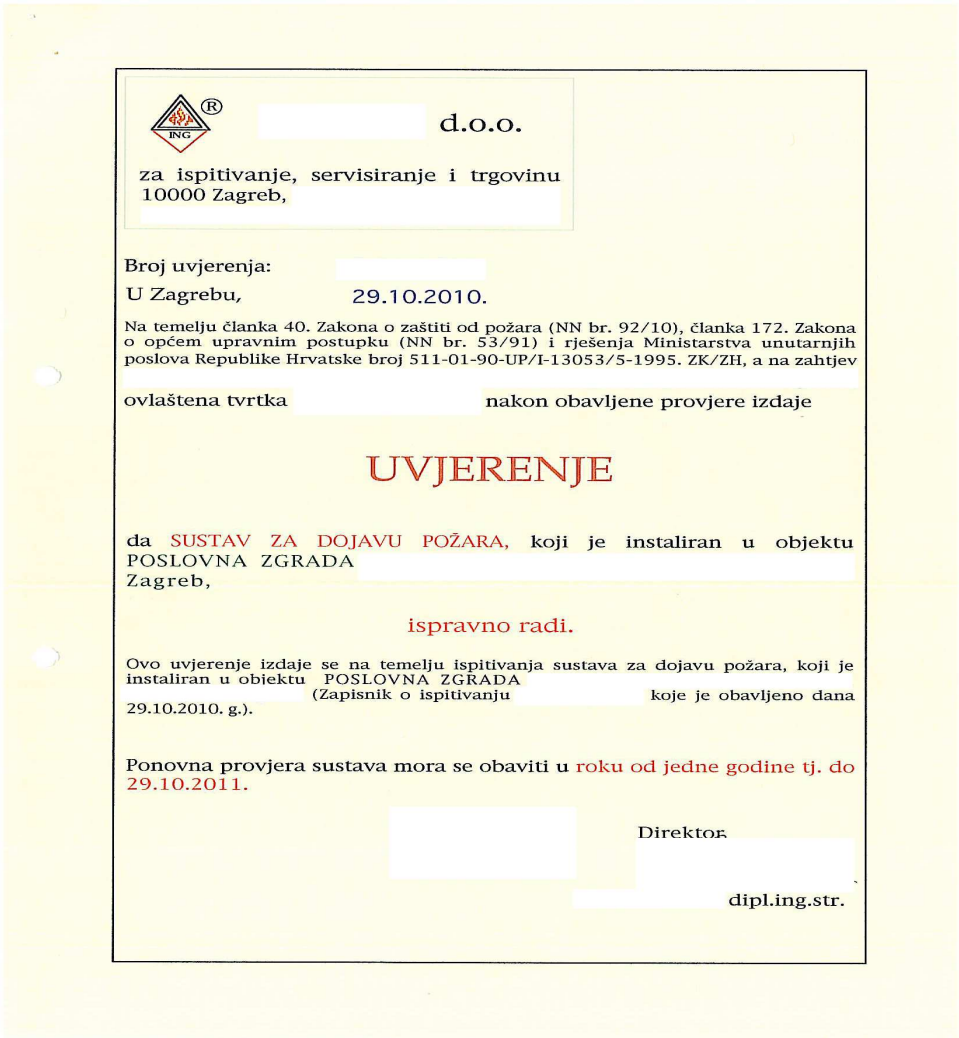
2.3.3. Vatrodojavni sustav

Vatrodojavni sustav (slika 15) na promatranim objektima koncipiran je na dvije vrste centralnih uređaja. Ovisno o veličini objekta implementirane su ili klasična vatrodojavna centrala ili na većim objektima analogno-adresabilna vatrodojavna centrala. Na svim objektima vatrodojavni sustav izveden je na način da je centrala smještena u „tehničkoj sobi“ koja je zbog toga izrađena kao zasebni požarni sektor. Svaka vatrodojavna centrala spojena je preko komunikatora u protuprovalnoj centrali na 24 satni tehnički nadzor i to dojava požara i greške vatrodojavne centrale. Na izdvojenom mjestu postavljen je upravljački LCD display s prikazom statusa vatrodojavne centrale. Ovo je izvedeno samo na objektima sa implementiranom analogno-adresabilnom vatrodojavnom centralom. Posebno se štite centralne server sobe u kojima se implementira sustav s visokom osjetljivošću (aspiracijski sustav za uzorkovanje zraka) koji potom aktivira sustav gašenja plinom.



Slika 15: Predodžba vatrodojavnog sustava

Na nekim velikim objektima visoke kategorije ugroženosti od požara postoji i vatrogasna služba koja prati rad vatrodojavnog sustava i bavi se preventivnom zaštitom od požara.



d.o.o.

za ispitivanje, servisiranje i trgovinu
10000 Zagreb,

Broj uvjerenja:

U Zagrebu, 29.10.2010.

Na temelju članka 40. Zakona o zaštiti od požara (NN br. 92/10), članka 172. Zakona o općem upravnim postupku (NN br. 53/91) i rješenja Ministarstva unutarnjih poslova Republike Hrvatske broj 511-01-90-UP/I-13053/5-1995. ZK/ZH, a na zahtjev

ovlaštena tvrtka nakon obavljene provjere izdaje

UVJERENJE

da SUSTAV ZA DOJAVU POŽARA, koji je instaliran u objektu POSLOVNA ZGRADA
Zagreb,

ispravno radi.

Ovo uvjerenje izdaje se na temelju ispitivanja sustava za dojavu požara, koji je instaliran u objektu POSLOVNA ZGRADA
(Zapisnik o ispitivanju koje je obavljeno dana 29.10.2010. g.).

Ponovna provjera sustava mora se obaviti u roku od jedne godine tj. do 29.10.2011.

Direktor

dipl.ing.str.

Slika 16: Predodžba uvjerenja o funkcionalnosti sustava

Svi vatrodojavni sustavi redovno se održavaju dva puta godišnje, a jednom se izvodi periodički godišnji pregled od ugovorenog ovlaštenog partnera. Svi nalazi s redovnih pregleda upisuju se u knjigu održavanja, a o godišnjem periodičkom ispitivanju ovlaštena tvrtka izdaje uvjerenje o funkcionalnosti sustava (Slika 16).

2.3.4. Sustav kontrole prolaza

Sustav kontrole ulaza izveden je od istog proizvođača na svim objektima. Ovako se mogu uvijek koristiti iste kartice a sustav je objedinjen u zajedničku bazu podataka s praćenjem na centralnom mjestu. Sustav je koncipiran na kontrolerima razmještenim po objektu (slika 17).

Slika 17 : Predodžba kontrolera kontrole pristupa

Svaki kontroler može upravljati s 2 čitača (slika 18) beskontaktnih kartica (jedna vrata obostrano ili dvoja vrata jednostrano).

Slika 18: Predodžba čitača kontrole pristupa

Kontroleri su povezani UTP kabelom na vlan tehničke zaštite. Aplikacija za upravljanje kontrolerima nalazi se na virtualnim serverima dok je baza izdvojena na database serveru. Svi serveri i baza su u redovitom procesu backupa.
Kontroleri posjeduju autonomno napajanje tako da rade i prilikom nestanka električne energije. Svaki je proširiv s dodatnim relejnim izlazima pa se po potrebi mogu izvesti razne međuovisnosti među pojedinim vratima ili vremensko zatezanje

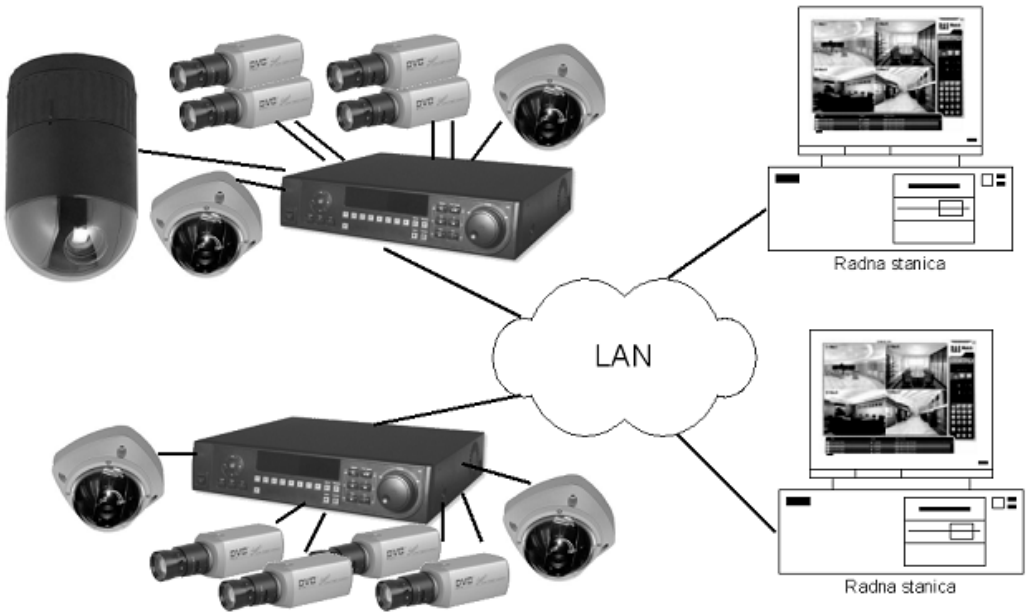
Slika 19: Predodžba čitača otiska prsta

otvaranja vrata. Za prolazak se koriste beskontaktne kartice tipa LEGIC kojima se programiraju posebni pristupni nivoi za svakog djelatnika zasebno. Sustav konstantno prati otvorenost vrata tako da u slučaju nasilnog otvaranja (bez autorizacije karticom) odmah dojavljuje alarmni signal na dojavni centar. Isto se događa i kada vrata ostanu otvorena duže nego što je to programski omogućeno.
Na vratima koja su predviđena za evakuaciju projektom je predviđeno da se ugradi „fail safe“ elektroprihvatnik koji u slučaju aktivacije vatrodojave ostavlja vrata u otvorenom stanju. Osim ovog, pokraj svakih vrata postavljena je kutija za čuvanje ključa za evakuaciju do kojeg se može doći razbijanjem stakla priloženim čekićem. Kutija za ključ spojena je na protuprovalni sustav i dojavljuje signal razbijanja stakla na dojavni centar.

Prostori od posebne važnosti kao regionalni trezori i server sobe produkcijskog i backup okruženja dodatno su štićeni biometrijskom kontrolom prolaza. Za ulazak u takve, posebno štićene prostore implementiraju se čitači otiska prsta (slika 19).

2.3.5. Sustav video nadzora

Sustav video nadzora (slika 20) temelji se na digitalnom video snimaču koji pohranjuje zapise na tvrdi disk u digitalnom obliku. Uglavnom se koriste analogne video kamere osim u posebnim slučajevima kada je potrebno više detalja za kasniju analizu, tada se koriste megapixelne IP kamere.



Slika 20: Predodžba sustava video nadzora

Bitne značajke digitalnog snimača su:

- Detekcija pokreta u slici
- Arhiva video zapisa minimalno 7 dana
- Minimalno 10 slika u sekundi
- Pregled pohranjenog video zapisa na monitoru bez prekidanja pohrane
- Izbor više različitih načina prikaza na monitoru (slijedni, više kamera istovremeno
- Spajanje na mrežni sustav i pregled snimača preko WEB sučelja

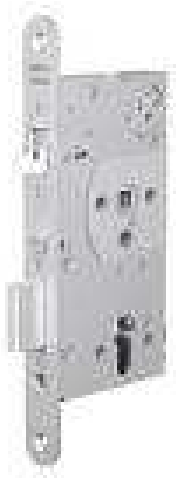
- Vremenska sinkronizacija sa vremenskim serverom
- Mogućnost snimanja video zapisa na vanjski medij
- Nekoliko video ulaza i izlaza za integraciju sustava
- Mogućnost spajanja pokretnih kamera
- Mogućnost slanja mail poruke o događajima i statusu snimača

Svaki snimač mora dojaviti na dojavni centar gubitak video signala sa kamere ili neki od kvarova sustava, kao i imati mogućnost da po signalu sa provalne centrale u slučaju alarma pokrene brže snimanje, ili okrene pokretnu kameru u određeni položaj. Napajanje za kamere izvodi se sa posebnim napajanjem koji posjeduje rastalni osigurač za svaku pojedinu kameru, a napajanje kao i video snimač spojeni su na UPS koji omogućava autonomiju rada u projektom zadanom vremenu.

U poslovnicama kamerama su pokriveni vanjski i unutarnji perimetar, put dostave novca, prostor za rad s klijentima, trezor, tehnička soba, arhiva, diskretna blagajna, brojačnica novca, i samouslužni uređaji. Konceptom zaštite propisan je način montaže i pokrivanja procesa kamerama međutim puno detalja ostavljeno je na odluku direktnom instalateru što u konačnici nije dobro jer ne postoji jedinstven pristup podešavanju kamera i snimača (misli se na širinu kadra, broj slika u sekundi za pojedinu kameru, rezoluciju snimanja, područje izuzeto od detekcije pokreta, osjetljivost detekcije pokreta i sl.).

2.3.6. Sustav mehaničke zaštite

Sustavom mehaničke zaštite smatraju se razne fizičke barijere, rešetke, protuprovalna vrata, protuprovalne brave i sl. Na promatranim objektima uglavnom se ugrađuju protuprovalna vrata s elektroprihvatnicima ili posebnim elektroničkim sigurnosnim bravama (slika 21) koja su kontrolirana kontrolom pristupa.



Slika 21: Predodžba električne sigurnosne brave

Prostori gdje se nalaze kase, predprostori soba s kasama i ulaz u diskretnu blagajnu ugrađena su protuprovalna vrata ili rešetke i električna cilindar visokog stupnja mehaničke čvrstoće (slika 22).

Slika 22: Predodžba električnog cilindra

Slika 23: Predodžba interlocking balističkih vrata

Poslovi mehaničke zaštite ugovoreni su s bravarskom tvrtkom koja posjeduje licencu za obavljanje poslova privatne zaštite sukladno zakonu. Na sva vrata koja su štićena kontrolom ulaza i na glavni i sporedni ulaz u objekt ugrađeni su sigurnosni cilindri čije ključeve izrađuje također samo ugovoreni partner.

Osim navedenih elemenata pod mehaničkom zaštitom smatraju se i same kase koje moraju biti odgovarajućeg stupnja otpornosti od provale o čemu se izdaje certifikat. Također na novije izvedenim poslovnicama implementiran je protubalistički zid oko prostora s kasom, i oko diskretne blagajne. Na ovaj način pristup gotovini je prilično otežan i na objektima štićenim na ovaj način Ministarstvo može donijeti odluku o oslobođenju od tjelesne zaštite kao mjere sigurnosti ne objektu.

Na nekim poslovnicama instalirani su sustavi interlocking balističkih vrata (slika 23)koja propuštaju samo jednu osobu istovremeno, a mogu se i blokirati u slučaju prepadnog alarma. Na ovako štićenim objektima također nije potreban zaštitar.

2.3.7. Tjelesna zaštita

Na manjem broju poslovnica promatrane institucije, osim u 24 satnim poslovnicama zakonska je obaveza imati tjelesnu zaštitu pa je ona i prisutna. Usluga pružanja tjelesne zašite ugovorena je s više vanjskih strateških partnera koji osiguravaju zaštitare na objektima, dostavu gotovog novca, eventualnu potrebu za vatrogascima i zaštitom javnih manifestacija te uslugu dojavnog centra sa 24 satnom intervencijom u slučaju alarma. Na većini objekata od MUP-a je dobivena suglasnost na prosudbu ugroženosti koja je utvrdila da tjelesna zaštita nije potrebna odnosno da je sigurnost povećana drugim mjerama kao što su balistički odvojena kasa, ili sustav cijevne pošte, interlocking vrata i dr. Zaštitari na velikim objektima prisutni su 24 sata, a na ostalima samo u radno vrijeme. Na svim objektima postoji soba u kojoj zaštitari imaju sef za pohranu oružja i ta prostorija se štiti protuprovalnim i protupožarnim sustavom. Za sve zaštitare propisani su standardom postupci pri kojima moraju biti aktivno uključeni a to su:

- dotacija gotovog novca u poslovnicu
- punjenje bankomata od strane djelatnika poslovnice
- dostava nova na gotovinska radna mjesta
- servisiranje bankomata
- pražnjenje dnevno-noćnog trezora i brojača kovanica od strane djelatnika poslovnice
- korištenje sefova građana
- odvoz suviška gotovog novca iz poslovnice
- sve najavljene veće isplate gotovine propisane posebnom Uputom

- prilikom svakog ulaska u sobu s kasom od strane stranih osoba, servisera i sl.

Za vrijeme svoje smjene svaki zaštitar obavezno zadužuje bežično panik tipkalo koje mora sa sobom nositi. Njime može pozvati interventnu ekipu u pomoć u slučaju potrebe.

Veliku sigurnost od napada razbojnika na dostavu novca osiguravaju implementirani sustavi spremnika s kemijskom zaštitom. Naime, u svakom spremniku u kojem se prenosi gotovina nalazi se spremnik sa bojom koji se u slučaju nasilnog otvaranja, ili ispuštanja iz ruke na mjestu koje nije za to predviđeno aktivira i uništi sav novac. Ovo vrlo dobro preventivno djeluje na razbojstva a osigurava pošiljke i od sabotaže od strane djelatnika zaštitarske tvrtke jer niti oni ne mogu otvoriti spremnik. Spremnik se otvara tek kada stigne u sami trezor poslovnice i zadovoljeni su svi uvjeti za njegovo otvaranje. Potom se puni ili prazni i ponovno je pri izlasku zaštićen od razbojstva.

2.4. Analiza postojećih sustava zaštite na bankomatima

Zaštita bankomata naočigled je prilično jednostavna zbog male površine mogućeg ugrožavanja ali iz istog razloga ovaj element je potrebno posebno zaštititi jer se na malom mjestu nalazi velika količina gotovog novca. Lokacije postavljanja bankomata su razne trgovine, knjižnice, i drugi prostori koje nisu i nemaju mogućnost biti zaštićeni od provale tako da bankomat mora imati implementiran svoj sustav zaštite, i pored toga mora obavezno biti osiguran od odnošenja sidrenjem u pod.

Na promatranim objektima zaštita je izvedena u skladu sa zakonom. Na svim bankomatima implementiran je protuprovalni sustav koji je podijeljen na 2 podsistema. Gornji dio bankomata posebna je particija zaštite i za isti šifru imaju serviseri informatičke opreme kako bi mogli nesmetano obaviti servis na bankomatu kao što je otklanjanje kvara, zamjena potrošene trake u printeru itd. Za donji, trezorski dio, šifre protuprovalnog sustava imaju samo osobe koje pune bankomat i one se periodički mijenjaju. Bankomat je štićen od provale kontaktima koji detektiraju otvaranja bilo kojeg dijela, i detektorima šuma koji detektiraju udarce, rezanje brusilicom ili povećanje temperature. Od izvršnih elemenata ugrađene su po dvije sirene, unutarnja i vanjska koja čak ima mogućnost dojave sabotaže od otvaranja ili punjenja stranim tijelom. Dojava alarmnih signala je najvažnija točka zaštite a u skladu sa zakonom mora se osigurati njena 24 satna nadziranost. Ovo je izvedeno na način da je protuprovalni sustav na dojavni centar spojen LAN konekcijom koja je konstantno nadzirana. Čim de dogodi greška u komunikaciji dojava se prenosi preko alternativnih komunikacijskih kanala (telefonska linije, GSM komunikatora) te se odmah upućuje interventna ekipa u kontrolu. Promatrani investitor uvidio je važnost što ranije detekcije pokušaja provale tako da se prilikom implementacije sustava zaštite na bankomatu obavezno štiti i prostor najmodavca naravno u dogovoru sa istim čime se postiže dodatna sigurnost. Bankomati se prema važećim propisima održavaju redovnim servisnim pregledima jednom godišnje o čemu se vodi evidencija.

2.5. Analiza postojećih sustava zaštite na objektima od posebne važnosti

Pod objektima od posebne važnosti smatramo regionalne trezore i nekoliko rezidencijalnih objekata članova uprave financijske institucije. Ovi drugi posebni su zbog visokog stupnja tajnosti i diskrecije prilikom implementacija i kasnijeg održavanja sustava.

Regionalni trezori vrlo su specifični zbog procesa koji nisu uobičajeni za ostale institucije kao što su brojanje novca, pakiranje novca za bankomate, dovoz i odvoz velikih količina novca i dr. Kako je svaki trezor specifičan zbog svoje građevinske konstrukcije i zbog različitog prilaza vozila na licu mjesta se dogovaraju posebne mjere zaštite već prije projektiranja sustava. One su uglavnom bazirane na temeljnim pravilima kao i ostale poslovnice što se tiče opreme i samog parametriranja sustava uz nekoliko dodataka. Prije svega zidovi trezora već prilikom građevinskog projektiranja moraju zadovoljiti čvrstoćom i neprobojnošću u određenom vremenu. Također sva vrata moraju biti protuprovalna ili čak protubalistička. Na glavnom ulazu obavezan je detektor metala a ulazi u posebno štićeni prostor sa kontroliranim vratima moraju tražiti dvostruku autorizaciju (potrebna je i kartica i biometrija u obliku otiska prsta da bi se korisnik propustio). Na svim zidovima, stropovima i u podu samog trezora u kojem se čuva gotovina ugrađuju se detektori šumova. Na mjestu primopredaje novca od strane zaštitarske tvrtke mora biti ugrađen protubalistički pult kroz koji se zaprimaju pakiranja sa gotovim novcem. On mora imati dvije mehaničke pregrade koje se ne smiju moći otvoriti niti u jednom trenutku istovremeno. Na ovaj način ovo oslabljeno mjesto je zaštićeno od ulaska osoba kroz pult. Osim ove mjere također i rolo vrata za ulaz u garažu moraju biti zatvorena kako bi se pult mogao otvoriti.

Posebnu pažnju pri zaštiti regionalnih trezora promatrani investitor posvetio je sustavu video nadzora koji je u njih implementiran. Osim klasičnog sustava kao u ostalim objektima određene procese potrebno je dodatno snimiti visokom rezolucijom i u realnom vremenu pa su na objektima ugrađene mrežne megapikselne kamere. Njima su pokriveni svi važniji procesi u kojima se nalazi

gotov novac pa tako imamo kameru na svakom primopredajnom pultu, iznad svakog brojača novaca, i iznad svakog punioca novca u ladice za bankomate. Kamere su povezane u zasebnu kompjutersku mrežu kojom upravlja mrežni preklopnik smješten u tehničkoj sobi regionalnog trezora. Video zapisi snimaju se na mrežnom video snimaču koji odgovara karakteristikama. Snimačima je moguć pristup preko mreže sa izdvojene lokacije. Ovim kamerama snima se puno više detalja pa se kasnije slike mogu bolje digitalno povećavati i obrađivati a osim rezolucije bitna je i brzina snimaka koja mora biti u realnom vremenu (24 slike u sekundi) jer se procesi brzo odvijaju.

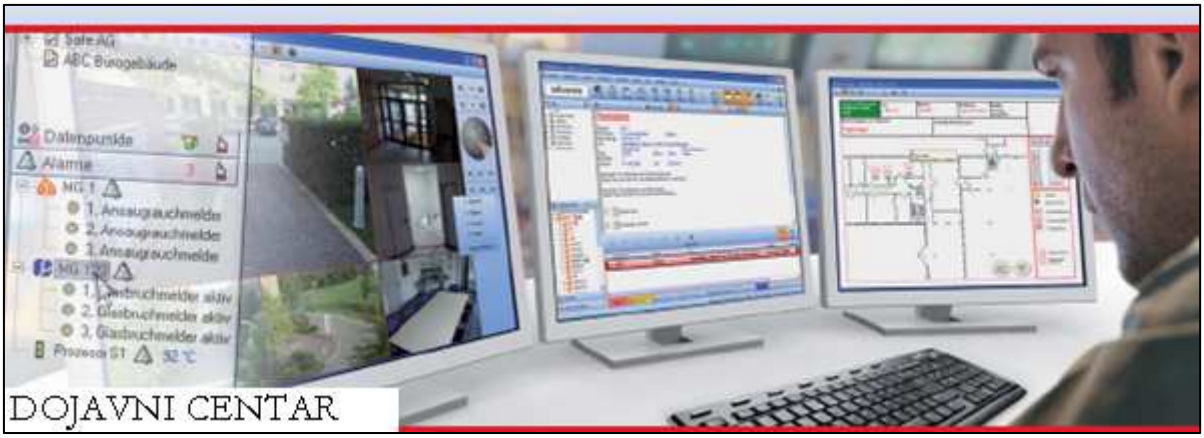
O svim procesima potrebno je izraditi procedure korištenja i o njima treba upoznati sve osobe na objektu. Navedeno je sukladno konceptu zaštite obaveza projektanta a reviziju procedura obavlja nadzor u suradnji s izvođačem na samoj primopredaji sustava.

2.6. Analiza postojećih sustava zaštite na velikim objektima

Pod velikim objektima smatraju se objekti u kojima je smještena logistika financijske institucije, skladišta materijala, razne popratne službe, arhive i dr. Ovi objekti nalaze se na nekoliko mjesta i na njima su također implementirani sustavi tehničke zaštite. Sustavi se razlikuju od ostalih jedino po tome što su koncipirani za nadzor sa centralnog mjesta jer na svakom velikom objektu postoji tjelesna zaštita u obliku zaštitara na recepciji. Na mjestu 24 satnog dežurstva nalazi se monitor za praćenje bitnih kamera za nadzor objekta, kao i upravljačka tipkovnica protuprovalnog i vatrodojavnog sustava. Osim ovih razlika bitno je reći da na velikim objektima ne postoji jedinstvena odgovorna osoba jer su u objektu nalazi mnogo različitih organizacijskih jedinica čime je veliki dio odgovornosti prepušten direktnom izvođaču implementacije sustava i kasnijeg održavanja istog. Kako nema velikog ugrožavanja od razbojstava jer uglavnom nema gotovog novca na samom objektu sustavi prilagođeni samo za zaštitu perimetra, a kontrola prolaza ugrađena je samo na bitnijim mjestima kao što su elektronske arhive ili ulazi iz jednog sektora u drugi.

2.7. Daljinski nadzor i postupanja kod alarmnih stanja

Svi sustavi tehničke zaštite na objektima promatrane financijske institucije spojeni su preko digitalnih komunikatora na Centralni dojavni sustav (CDS).
Ova usluga 24 satnog praćenja ugovorena je sa tvrtkom koja može u svakom trenutku po dojavi alarmnog stanja sa objekta na isti odmah uputiti interventnu ekipu ili potrebnu pomoć ovisno o vrsti signala. Usluga je ugovorena za područje cijele Republike Hrvatska.



Slika 24: Predodžba CDS-a

Svi događaji koje CDS (slika 24) može zaprimiti razvrstani su u nekoliko osnovnih skupina i za svaku je procedurom utvrđen redoslijed postupaka za operatera na dojavnom centru.

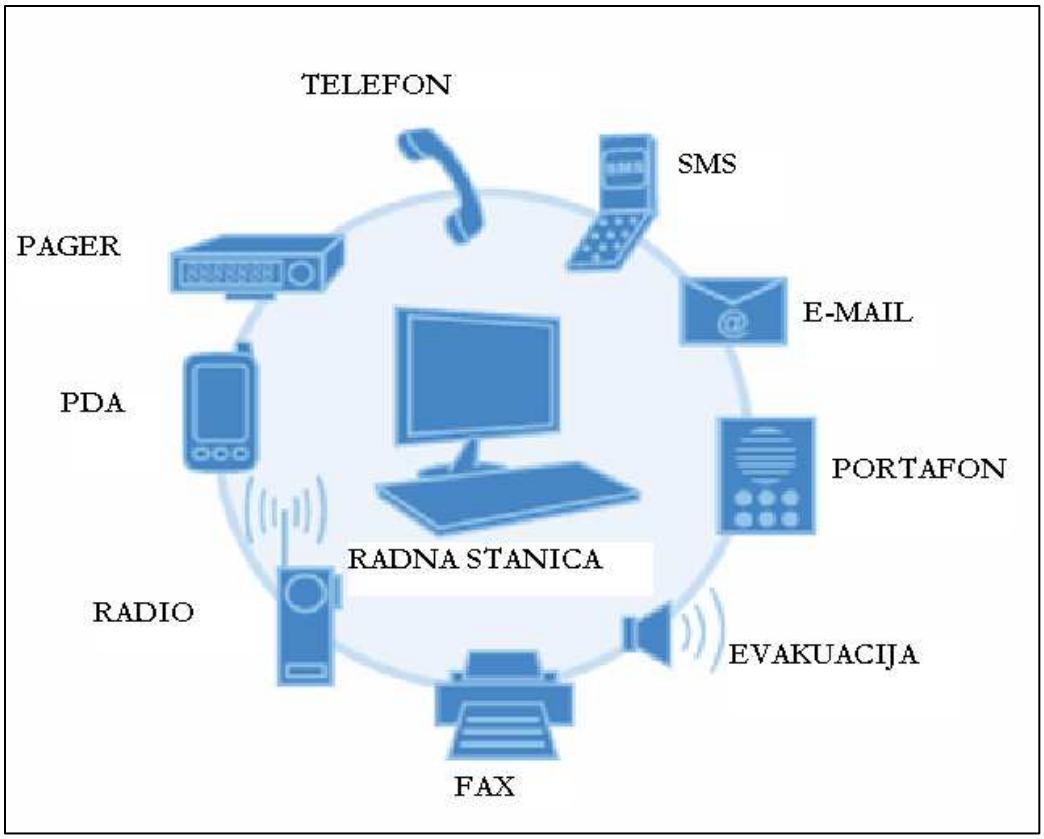
Signali koje CDS može razlikovati su svrstani u slijedeće skupine:

- PROTUPREPADNI ALARM (panik tipke, panik šine, bežične panik tipke i šifra prisile)
- PROTUPROVALNI ALARM (detektori kretanja, šuma, loma stakla i magnetski kontakti na vratima)
- ALARM SUSTAVA KONTROLE PROLAZA (vrata nasilno ili predugo otvorena - magnetni kontakt)
- SABOTAŽNI ALARMI (opreme sustava tehničke zaštite)
- POŽARNI ALARM (sustava dojave požara)
- TEHNIČKI ALARM
  a. (nestanak napajanja el. energijom napona 220V i nizak napon akumulatora)
  b. (gubitak komunikacije)
  c. (gubitak video signala)
  d. (DAT traka puna)
  e. (ostali tehnički alarmi)
- TEHNOLOŠKI ALARMI (javljači poplave i povećane temperature; nepravilnosti na objektu, oštećenja staklenih površina, oštećenja ulaza, itd.)
- KONTROLA UKLJUČIVANJA/ ISKLJUČIVANJA SUSTAVA TZ SVAKOG POJEDINOG OBJEKTA

Signali koji se dojavljuju po prioritetima su razvrstani i za svaki od njih propisana je procedura postupanja i to za slučaj u toku i izvan radnog vremena poslovnice sa koje je signal stigao. Po navedenoj proceduri neke signale nije moguće opozvati npr. protuprepadni alarm a neke je uz telefonsku identifikaciju lozinkom preko telefona. Postoji nekoliko tipova komunikacije dojavnog centra sa korisnikom (slika 25).

Osiguranje 24 satnog nadzora nad komunikacijom sa dojavnim centrom osigurano je implementacijom LAN modula na protuprovalnoj centrali koji odmah po prekidu komunikacije dojavljuje kvar preko alternativnih komunikacijskih kanala. U slučajevima gdje ne postoji LAN veza sa dojavnim centrom centrala je

programirana da jednom dnevno prenese jedan test komunikacije uvijek u isto preprogramirano vrijeme. U slučaju izostanka ovog testa CDS postupa kao i za svaki sabotažni alarm odnosno šalje interventnu ekipu koja osigurava objekt do obnove komunikacije.



Slika 25: predodžba tipova komunikacije dojavnog centra

Posebnom procedurom propisano je postupanje po dojavama sa eksternih bankomata jer oni su dostupniji i više podložni sabotažama sustava tehničke zaštite. Sa eksternih bankomata se razlikuju slijedeći alarmni signali:

- Alarm ulazno/izlazne zone particije korisnika prostora
- Alarm ulazno/izlazne zone particije bankomat
- Alarm otvaranja donjeg dijela bankomata
- Alarm detektora šuma na bankomatu
- Alarm sabotaže (sirene, centrale, detektora)
- Panik alarm s tipkovnice u particiji bankomat
- Požarni alarm s tipkovnice u particiji bankomat i detektora požara

- Tehnički alarm – nestanak napajanja el. energijom napona 220V i nizak napon akumulatora
- Gubitak komunikacije s mreže bankomata
- Prekid komunikacije sa sustava TZ – izostanak testa
- Dojave tehničkih grešaka na sustavu
- Kontrola uključenja/isključenja
- Tehnološki alarmi (oštećenja tipkovnica ili ekrana bankomata – dojava dolazi od policije ili klijenata, a nije proradila TZ)

Za svaki od navedenih alarma također je procedurom određeno postupanje operatera na CDS-u kao i interventne ekipe. Bitno je da CDS uvijek posjeduje ažuriran popis osoba sa svim njihovim kontaktima koje mora obavijestiti u slučaju prorade alarma. Ovdje se prvenstveno misli na vlasnike prostora u koje je smješten bankomat kao i na odgovorne osobe za punjenje i servisiranje bankomata.
O svim događajima sa objekata institucije CDS je sukladno ugovoru dužan redovito izvještavati sektor upravljanja sustavom zaštite i to kroz ugovorena dnevna, tjedna , mjesečna, kvartalna, godišnje te po potrebi izvanredna izvješća .Pored navedenih izvješća instituciji je omogućen uvid u trenutna događanja putem direktne veze sa nadzornim centrom. Forma izvješća propisana je od strane investitora i prilog je ugovoru o poslovnoj suradnji za predmetno područje.

2.8. Aktivnosti vezane za implementaciju sustava

Sukladno pravilniku o uvjetima i načinu provedbe tehničke zaštite podrazumijeva:

- snimku postojećeg stanja štićenog objekta i analizu problema s ocjenom;
- izradu prosudbe ugroženosti;
- izradu sigurnosnog elaborata;
- definiranje projektnog zadatka;
- projektiranje sustava tehničke zaštite;
- izvedbu sustava tehničke zaštite;
- stručni nadzor nad izvedbom radova;

- obavljanje tehničkog prijama sustava tehničke zaštite;
- održavanje i servisiranje sustava tehničke zaštite;
- uporaba sustava tehničke zaštite.

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

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

- Prosudba ugroženosti i elaborat mjera sigurnosti
- Izvedbeni projekt sustava tehničke zaštite
- Projekt izvedenog stanja

2.8.1.1 faze izrade prosudba ugroženosti i elaborata mjera sigurnosti

Bitan dio projektiranja sustava tehničke zaštite je prosudba ugroženosti jer se sve kasnije nadovezuje na istu a iz nje proizlazi i kategorizacija objekta koja nameće određene mjere zaštite. Izrada prosudbe ugroženosti izvodi se na bazi općih i posebnih podataka o predmetnom objektu. Ti podaci se odnose na: vrstu, namjenu i izgled, veličinu, broj prostorija, smještaj objekta (lokacija) i položaj u odnosu na okruženje, pristupne putove objektu, opća građevinska obilježja, postojeću infrastrukturu, blizinu policije, vatrogasaca ili zaštitarskih tvrtki, vrstu aktivnosti koje se u objektu obavljaju, visinu vrijednosti robe koja se u objektu nalazi, broj ljudi koji se povremeno ili stalno nalaze u objektu. Prosudba ugroženosti izrađuje se primjenom priznatih pravila u provedbi tehničke zaštite. Priznata pravila u

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

Iznimno u slučaju manjih nadogradnji moguće je izraditi samo izvedbena skica dogradnje sustava ali se kasnije promjene moraju evidentirati u projektu izvedenog stanja.

2.8.1.1.1 priprema projekta

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

2.8.1.1.2 prikupljanje podataka

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

2.8.1.1.3 obrada prikupljanih podataka

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

2.8.1.1.4 pisanje izvješća

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

2.8.1.1.5 prijedlog mjera

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

Izvedbeni projekt mora sadržavati točne dispozicije elemenata sustava tehničke zaštite, raspored opreme u tehničkoj sobi objekta kao i sve bravarske i stolarske elemente na koje su ugrađuju elementi zaštite.
Osim navedenog još se za svaku poslovnicu posebno izrađuje skica izvedenog stanja 24 satne poslovnice u kojoj moraju biti ucrtane mikrolokacije svih samouslužnih uređaja sa oznakama vrste i elementima tehničke zaštite koji se na njih montiraju.

2.8.2. Izvođenje

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

2.8.3. Nadzor nad izvođenjem

Sukladno Zakonu o privatnoj zaštiti poslove nadzora nad izvođenjem radova tehničkih zaštitnih sustava, revizije projektne dokumentacije tehničkih zaštitnih sustava, tehničkog primitka te pružanja intelektualnih usluga u području tehničke zaštite može obavljati zaštitar – tehničar koji ima završenu visoku stručnu spremu. Promatrana institucija ugovorila je posao stručnog nadzora sa dvije tvrtke koje imaju ovlast za ovakve poslove. Njihova zadaća je da prate svaku implementaciju sustava već od samog pregleda izvedbenih projekata i uvođenja instalatera u posao pa do primopredaje sustava i verifikacije okončanog financijskog razračuna. Nadzor nad izvođenjem uključuje:

- Nadzor nad implementacijom u smislu poštivanja pravila struke i Zakona
- Praćenje terminskog plana izvođenja i usklađivanju radova sa ostalim izvođačima na gradilištu
- Izvještavanje investitora o stanju na svim objektima koje nadzire u obliku tjednih izvješća
- Nadzor nad poštivanjem koncepta zaštite po kojem se sustavi moraju izvoditi
- Nadzor nad provođenjem mjera zaštite od požara i zaštite na radu prilikom implementacije sustava
- Sudjelovanje u primopredaji sustava te prikupljanje sve potrebne dokumentacije i atesta za opremu
- Tehnički pregled izvedenih radova te kontrole otklanjanja nedostataka u zadanom vremenu
- Upisivanje tijeka radova i komentara nadzora u građevinski dnevnik

- Sudjelovanje u koordinaciji prilikom izmjena u projektu

- Pregled utrošeno materijala i opreme kao i financijska verifikacija okončanih situacija

2.8.4. Primopredaja sustava

Po obavljenoj implementaciji a prije početka korištenja sustava mora se sukladno Zakonu izvršiti primopredaja sustava. Ovo izvode predstavnici izvođača, investitora i ugovorenog nadzora nad izvođenjem. U sklopu primopredaje izdaju se potvrde o obuci korisnika, popis kartica kontrole pristupa sa pristupnim nivoima, popis sigurnosnih ključeva, te se predaju svi certifikati za opremu.
Nakon izvršene primopredaje izvođač izdaje vlasniku ili korisniku objekta potvrdu da je sustav tehničke zaštite izveden sukladno odredbama Pravilnika o uvjetima i načinu provedbe tehničke zaštite. Sastavni dio potvrde (prilog 2) je i zapisnik (prilog 3) o obavljenom tehničkom prijemu, a propisani obrazac za oba dokumenta dan je u pravilniku. Na potvrdu se upisuje kategorija objekta sukladno Pravilniku koju je odredio projektant sustava u sklopu prosudbe ugroženosti. U zapisnik nadzor upisuje eventualne nedostatke na sustavima i rok za njihovo otklanjanje a potvrdu njihovog otklanjanja mora također nadzor verificirati ponovnim pregledom.

2.8.5. Održavanje i uporaba

Sukladno Zakonu o privatnoj zaštiti sustavi tehničke zaštite moraju se održavati jednom godišnje. Poslove održavanja investitor je dužan ugovoriti sa tvrtkom licenciranom za poslove tehničke zaštite a tvrtka je dužna sukladno ugovoru izdati zapisnik o redovnom pregledu, i upisati stanja svih sustava u knjigu održavanja. Analizirana institucija poklanja dosta pažnje redovnom održavanju pa se odlučila za 2 pregleda godišnje za sve objekte i jedan za bankomate. U sklopu ugovora o održavanju dan je popis svih lokacija objekata i bankomata i propisani su radovi koji se izvode prilikom redovnog održavanja. U nastavku (tablica 3) je primjer „chek liste“ sa komentarima koja se ispunjava prilikom redovnog održavanja.

Tablica 3: kontrolna lista redovnog održavanja sa specifikacijom radova

	redovni servis opis radnji	odrađeno	komentar - primjedba
1	Provjera funkcionalnosti sustava		
2	Provjera napajanja (glavno, pomoćno)		
3	Provjera ispravnosti optičke i zvučne signalizacije svih dijelova sustava		
4	Kontrola i podešavanje napona održavanja pričuvnog izvora		
5	Ispitivanje ispravnosti panik-tipki i panik-šina te daljinskih panik-tipki i njihovog dometa		
6	Provjera i podešavanje osjetljivosti javljača šuma		
7	Provjera i podešavanje kuta pokrivenosti prostornih detektora		
8	Regulacija dometa infracrvenim detektorima ukoliko je potrebna		
9	Provjera sabotažnih kontakata na svakom senzoru i ostalim dijelovima sustava		
10	Provjera spojnih mjesta na uređajima koji su izloženi stalnoj manipulaciji ili atmosferilijama		
11	Provjera komunikacije sa središnjim nadzornim sustavom ili nekim drugim dojavnim mjestom ako postoji		
12	Čišćenje senzora od taloga prašine ako postoji		
13	Čišćenje signalnog dijela centralnog uređaja i ostalih uređaja		
14	Provjera ispravnosti beskontaktnih čitača		
15	Kontrola PC-a za pohranu podataka		
16	Provjera spojnih mjesta u razvodnim ormarićima		
17	Provjera spojeva u centrali		
18	Ispitivanje vanjske i unutarnje sirene		
19	Ispitivanje telefonske dojave i provjera telefonskih brojeva		
20	Podmazivanje i podešavanje električnih brava		
21	Podmazivanje i podešavanje pumpi		
22	Čišćenje i provjera ispravnosti magnetskih čitača		
23	Čišćenje kućišta		
24	Čišćenje glave snimača		
25	Čišćenje objektiva		
26	Čišćenje stakalca		
27	Kontrola arhive video-zapisa radi uočavanja neispravnosti kamera		

28	Ispitivanje svih ionizacijskih, optičkih i termičkih javljača jednom godišnje		
29	Provjera veze s vatrogasnim centrom ili sa središnjim nadzornim sustavom		
30	Provjera obučenosti korisnika (dostaviti zapisnik)		
31	Upis obavljenih poslova u knjigu održavanja		
32	Usklađenost dokumentacije izvedenog stanja sa stvarnim stanjem na objektu		
33	Provjera smještaja alarmnih bljeskalica - ne smiju biti vidljive npr. kroz staklenu zidnu stijenu		
34	Provjera antimaskinga - da li je spojen i da li ide dojava u RDC		
35	Provjera definicije particija		
36	Provjera projektiranih preseta na pokretnim dome kamerama		
37	Provjera funkcionalnosti vanjske i unutarnje rasvjete, provjera noćnih snimki		
38	Provjera s RDC-om da li se prosljeđuju informacije o predugoj otvorenosti vrata i alarm interlockinga kase		
39	Provjera smještaja tipki za izlaz, da li su dostupne izvana npr. kroz rešetku na trezorskim vratima		
40	Postoji li tipka za blokadu kod prijenosa novca		
41	Provjera natpisa na interfonu, ne smiju ukazivati na funkciju onoga kome se zvoni npr. ne smije pisati glavni blagajnik		
42	Provjera duljine arhive video zapisa		
43	Provjeriti da li u poslovnici imaju procedure i potrebne zapisnike(zapisnik o tehničkom prijemu, korisničke upute).		

Osim navedenog održavanja izvođač je dužan osigurati održavanje i servisiranje sustava u jamstvenom roku, a na zahtjev korisnika ponuditi održavanje i servisiranje izvan jamstvenog roka, te omogućiti isporuku potrebnih pričuvnih dijelova u razdoblju pet (5) godina od dana puštanja sustava u rad.

2.9. Analiza i prijedlog poboljšanja mjera zaštite

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

2.9.1. Protuprovalni sustav

Na protuprovalnim sustavima u pravilu nema zamjerki odnosno implementirana oprema zadovoljava sve današnje potrebe no ipak mjesta za poboljšanje ima.

- Prvenstveno je potrebno sve protuprovalne centrale proširiti sa LAN modulima i svu komunikaciju ostvariti preko mrežne tehnologije a telefonske linije i GSM komunikatore staviti isključivo kao „backup“ ovoj vezi. Za ovu nadogradnju ostvareno je mnogo preduvjeta jer većina centrala podržava ovaj modul i mrežna infrastruktura je već u funkciji pa financijski gledano trošak nije velik. Na ovaj način osigurava se mnogo sigurnija komunikacija sa nadzornim centrom koji na ovaj način ima 24 satnu kontrolu nad komunikacijom što je već ionako obaveza za sustave na bankomatima sukladno Zakonu.

- Na velikim objektima zbog stalnih nadogradnji dogodilo se da je ugrađeno više protuprovalnih centrala na jednom objektu pa je otežano održavanje i snalaženje po sustavima. Navedene centrale je potrebno čim prije zamijeniti sa jednom koja može primiti na sebe sve particije na velikom objektu. Demontirana oprema može se upotrijebiti za održavanje i buduće nadogradnje po poslovnicama pa trošak ove nadogradnje također nije velik.

- U projektima treba definirati da li su alarmne zone detekcije nadzirane i sa koliko završnih otpornika kako bi svi sustavi bili jednoobrazno implementirani.

- Na bankomatima je potrebno spojiti detekciju otključanosti donjih vrata čime će se bankomat osigurati od sabotiranja djelatnika koji ga pune.

- Proceduralno je potrebno propisati da se sve šifre na protuprovalnim sustavima mijenjaju jednom godišnje prilikom redovnog pregleda sustava.

- Na svim objektima potrebno je jasno odvojiti particiju tehničke sobe te uspostaviti redoviti način uključenja zaštite u istoj. Ukoliko se zaštita u određenom vremenu ne postavi potrebno je uspostaviti automatsko uzbunjivanje dojavnog centra.

- Prilikom obilaska i pregleda objekata primijećeno je da antimasking funkcija na detektorima pokreta nije spojena kao zasebna zona detekcije nego više detektora u seriju pa se kasnije teško odredi koji detektor je izazvao alarm ove vrste. Potrebno je odvojiti antimasking detektora u zasebne zone detekcije dodavanje modula zonskih proširenja.

2.9.2. Protuprepadni sustav

- Na pojedinim lokacijama ugrađene su bljeskalice koje se aktiviraju nakon iniciranja protuprepadnog alarma. Ovo se obavezno treba izbaciti iz upotrebe jer može dovesti u opasnost osoblje u slučaju razbojstva. Isto se odnosi i na memoriju alarma na samoj panik tipki ili šini (LED).

- Osim navedenog potrebno je Konceptom odrediti tko treba posjedovati šifru prisile i za koje particije protuprovalnog sustava ona mora vrijediti, također i imaju li svi istu šifru ili se programira za svakog korisnika posebno.

- Prijedlog za poboljšanje zaštite od prepada je i ugradnja sustava kemijske zašite u ambalaže za pakiranje novca koje bi se aktivirale čim bi prijemnik na izlazu iz poslovnice izgubio signal od predajnika u ambalaži. Ovo je bitno jasno naznačiti naljepnicama na ulazu u poslovnicu da se preventivno djeluje na prepad.

2.9.3. Vatrodojavni sustav

Što se tiče sustava vatrodojavnih sustava oni su apsolutno zadovoljavajući obzirom da su ugrađeni i tamo gdje nisu obavezni kao mjera procjene ugroženosti od požara nego na zahtjev investitora. Jedina opaska dana je u smislu održavanja, naime na objektima se događaju česte promjene koje se ne upisuju u projekte izvedenog stanja pa se prilikom godišnjih periodičkih pregleda događa da su ispitivači u nedoumici odnosno ne izdaju potrebno uvjerenje. Uz ovaj događa se i problem na velikim objektima gdje zbog veličine objekta nije dovoljno dobar pregled aktivacije pojedinih javljača i izvršnih elemenata pa vatrogascima treba previše vremena da detektiraju točnu mikrolokaciju požara. Preporuka za poboljšanje je slijedeća:

- Dodane javljače ili novonastale prostorije bez javljača potrebno je odmah prijaviti strateškom partneru koji će uz pomoć nadzora ucrtati promjene u projekt izvedenog stanja vatrodojave.

- Prilikom većih nadogradnji sustava obavezno se mora od projektanta naručiti novi projekt izvedenog stanja, za isti zatražiti suglasnost od nadležnog tijela za zaštitu od požara te nakon toga funkcionalno ispitati sustav od ovlaštene ustanove.

- Na svim velikim objektima proširiti sustav nadzora nad aktiviranjem javljača sa centralnim računalom na kojem je moguće u trenutku aktivacije javljača vidjeti točnu mikrolokaciju detektora ili izvršnog elementa na mapi predmetnog prostora

- U sve prostore sa serverima dodatno ugraditi manji autonomni sustav gašenja aerosolom, ako su serveri u poslovnici isto implementirati u rack ormare. Ovime bi se dodatno zaštitili podaci u slučaju požara.

2.9.4. Sustav video nadzora

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

- Sve digitalne video snimače potrebno je umrežiti na centralnom mjestu osigurati dojavu kvara i otvoriti mogućnost fiksiranja video zapisa sa centralne lokacije. Na ovaj način troškovi izlazaka servisera zbog fiksiranja video zapisa bitno će se smanjiti a investitor će imati jedinstvenu bazu video arhiva za interne potrebe i potrebe policije. Ovakav sustav omogućuje i optimiziranje sustava sa centralne pozicije čim se promjene uvjeti snimanja na nekom od objekata.

- Potrebno je osigurati video zapis sa svih bankomata i navedeno spojiti na centralizirani video snimač, a u sliku sa bankomata integrirati tekst transakcije kako bi se uvijek mogla povezati slika i transakcija. Ovo nije velika investicija jer su mrežna veza, napajanje i centralna nadzorna soba već osigurani potrebno je samo preko WAN mreže proslijediti video signal i isti pohranjivati na jednom mjestu. Ovo otvara kasniju mogućnost proširenja na dojavu maskiranih i neprepoznatljivih osoba na bankomatu što se može učiniti naprednom video analizom i o tome obavijestiti nadzorni centar. Na slikama s bankomata mora se „ zamaskirati „ utipkavanje pina zbog zaštite tajnosti podataka.

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

- Konceptom nije detaljno dobro opisano parametriranje sustava video nadzora (kvaliteta zapisa, broj slika u sekundi.) pa sustavi nisu jednako parametrirani. Potrebno je detaljnije opisati zahtjeve investitora za pojedine vrste kamera i pozicije koje štite kako bi svi sustavi bili standardizirano programirani a ne prepušteni na volju instalatera.

- Na važnijim mjestima u poslovnicama instalirati megapikselne kamere koje osiguravaju kasniju bolju digitalnu obradu i analitiku snimljenog materijala. Pod važnijim mjestima predložena su: prostor kase i manipulacija novcem, brojanje novca, glavni ulaz u poslovnicu, izlaz novca iz cijevne pošte i bankomat.

- Potrebno je razmotriti ugradnju dodatnih reflektora koji bi osvjetljavali perimetar objekta. Također i unutarnja rasvjeta na nekim mjestima nije zadovoljavajuća pogotovo van radnog vremena, tako da za unutarnje kamere treba postojati minimalna nužna rasvjeta. Ovo je moguće riješiti ugradnjom IC reflektora, odnosno doradom razvodnih ormara rasvjete koja bi uvijek bila uključena.

- U slučajevima kada je na jednostavan način moguće doći do kamere odnosno tamo gdje su kućišta dovoljno nisko ili imaju mogućnost sabotaže potrebno je koristiti specijalna anti-vandal kućišta.

- Svim zaštitarima potrebno je osigurati računala na mjestu predviđenom za njihov boravak a ne ta računala potrebno je instalirati klijent aplikacije za mrežni pregled pojedinih kamera. Projektom je potrebno definirati koje kamere zaštitar smije pratiti.

2.9.4.1. Sigurnost video nadzora

U svijetu interneta i sveopće umreženosti, kada se tome pribroje sve brojniji sustavi video nadzora onda postaje jasno da nas se može nadzirati gotovo kamo god da se krećemo. Novčarske institucije posjeduju video nadzorne sustave koji su umreženi putem informatičke mreže. Upravo u umreženosti leži sigurnosni problem jer proizvođači opreme prodaju sustave video nadzora s omogućenim pristupom na Internet i na žalost prilično niskom razinom zaštite. Unatoč činjenici da sustavi videonadzora posjeduju mogućnost lozinke iste su tipizirane i solidno dokumentirane što znači da svi oni koji žele pristupiti sustavima video nadzora koji su priključeni na internet to mogu učiniti vrlo jednostavno, isprobavajući nekoliko tipiziranih lozinka. Istraživanjem obuhvaćeni su sustavi video nadzora ne samo banka već i trgovina, hotela, bolnica.

Kroz analizu sustava pokazalo se da su sustavi video nadzora loše zaštićeni zbog tvorničkih postavki sustava koji uključuju omogućen pristup s Interneta i jako slabe lozinke. Osim toga to znači isto da se za pristup takvim sustavima videonadzora ne moraju baviti hakeri jer pristupiti sustavima videonadzora može praktički bilo tko. Osim toga ranjivosti sustava pridonose i informacije objavljene na internetu na kojem je objavljena web stranica koja posjeduje poveznice brojnih nadzornih kamera koje nisu zaštićene. Moderniji i kvalitetniji sustavi jednako su podložni hakerskim napadima upravo zbog činjenice da se ne mijenjaju tvorničke lozinke i postavke. To omogućuje kontrolu nad video nadzorom. Međutim, spriječiti takve napade nije toliko složen koliko se na prvi pogled čini.

Prvi korak je poduzimanje mjera da se osobama za održavanje i upravljanje sustavima videonadzora prepusti da se sustav konfigurira prema pravilima struke. To znači da se najprije uklone tvorničke postavke, promijene podrazumijevane lozinke i pri tome promijene korisnička imena u nešto što će potencijalni napadači teže pogoditi. Za stjecanje kontrole na bilo kojim sustavima pa tako i na sustavima videonadzora koriste se maliciozne računalne skripte koje u vrlo kratkom periodu iskušavaju razne kombinacije lozinki i korisničkih imena pri čemu se prve isprobavaju tvorničke lozinke i korisnička imena. Jasno je da će sustav koji nema promijenjene tvorničke postavke biti vrlo brzo i bezbolno kompromitiran te kao takav može biti ulazna točka za pristup drugim dijelovima sustava.

Drugi korak je onemogućavanje pristupa sustavu s Interneta ili rekonfiguracija sustava. Obzirom da je udaljeni pristup vrlo koristan potrebno je rekonfigurirati sustav tako mu se može pristupiti isključivo iz lokalne mreže ili vpn-om. Takvom rekonfiguracijom sustav neće biti javno dostupan nego će biti dostupan samo ovlaštenim osobama.

2.9.5. Sustav kontrole prolaza i mehaničke zaštite

Kako sustavi kontrole prolaza zakonom nisu definirani do u detalje na predmetnim objektima svi sustavi su zadovoljavajući jer ispunjavaju uvjete za najzahtjevnije prostore koji su kategorije 1. po prosudbi ugroženosti. Kontrola pristupa na svakoj poslovnici detektira neovlašten ulazak i to dojavljuje na dojavni centar uz signalizaciju na licu mjesta. Također se na računalu pohranjuje baza prolazaka pa se kasnijim uvidom može pratiti tko je ulazio i kada u pojedini prostor. Uz interlock funkciju na ugroženijim vratima i vremensko zatezanje na ulazu u trezor sustav je na vrhu današnjih modernih tehnologija.

Prijedlozi za unaprjeđenje:

- Primijećeno je da je na pojedinim lokacijama tipku za izlaz iz predtrezorskog prostora (rešetke) moguće pritisnuti izvana pomoću duljeg štapa ili sličnog priručnog sredstva zbog čega je i izlaz i ovakvog prostora potrebno štititi čitačem kartica, a ne tipkalom za izlaz.

- Na sva ugroženija vrata (ulaz u predtrezor, ulaz u prostor sa kasom, stražnji ulaz u poslovnicu) potrebno je ugraditi električne brave a ne elektroprihvatnike kao što je sada ugrađeno. Ovime će se osigurati mehanička čvrstoća u slučaju pokušaja nasilnog otvaranja vrata

2.9.6. Tjelesna zaštita

Na promatranim lokacijama gdje djeluje tjelesna zaštita uočeno je da se prema pravilima struke izvršavaju sve procedure vezane na tjelesnu zaštitu.

Ono što je vrlo važno za napomenuti u analizi strukture zaposlenika u zaštitarskim tvrtkama, a čije usluge koriste financijske institucije jest selekcija, obuka i pozicioniranje zaštitara u bankama i utjecaj stresa na njih. Trebali bi pri tome biti ispunjeni određeni uvjeti dok u diskvalifikacijske okolnosti spada rad u više zaštitarskih tvrtki u kratkom vremenu, visoka materijalna zaduženost, život u nesređenim socijalnim okolnostima, nasilje u obitelji, neprimjeren vizualni izgled, nekultura ophođenja i pismenog izražavanja, nepoznavanje rada na računalu, niska razina higijene i kulture odijevanja, poroci poput alkohola, kocke, klađenja i slično, opravdani prigovori bivšeg poslodavca i moguće pokretanje prekršajnog ili kaznenog postupka.
Za preporučiti je nakon osnovne selekcije i odabira zaštitara za poslove zaštite u novčarskim institucijama da zaštitari prođu specijalističku edukaciju unutar koje je obuhvaćena edukacija o pravilima ponašanja u banci, ljubaznosti, uljudnosti, kulturi ophođenja sa strankama, klijentima, potom edukaciju u segmentu osnova verbalne i neverbalne komunikacije i komunikacije telefonom, razradu procedura postupanja u slučaju uporabe ovlasti od strane zaštitara.

2.9.7. Općenite mjere poboljšanja zaštite

- Ugovorom je potrebno definirati redovito ažuriranje procedura kretanja i prosudbi ugroženosti, definirati u kojim vremenskim razmacima je isto potrebno izvesti.

- Kod bilo kakvih promjena pozicije elemenata tehničke zaštite potrebno je te promijene evidentirati u projektu izvedenog stanja kako bi se uvijek znalo pravo stanje na objektu.

- Potrebno je uspostaviti sistem distribuiranja uputa zaštitarima, odgovornost za njihovu primjenu i način kontrole njihove primjene.

- Na velikim objektima obavezno treba imenovati osobu koja je zadužena za zaposlenike na objektu, njihovo ažuriranje (šifre, kartice, nivoi pristupa.) te potpisivanje izvještaja o učinjenim servisima i pokretanje zahtjeva za servisom. Sada se ovo radi neorganizirano odnosno svako može pokrenuti zahtjev a serviser ima odgovornost kome će dati koji pristupni nivo unutar objekta.

3. OSVRT NA NOVI ZAKON

U trenutku završetka pisanja ovog Završnog rada u redovitoj Saborskoj proceduri izglasan je novi Zakon o zaštiti novčarskih institucija. Novčarske ustanove, a osobito banke, slijedom prethodnih zakona vezanih za zaštitu novčarskih institucija, a i vlastitih želja za povećanjem sigurnosti, već su implementirale glavninu mjera traženih novim Zakonom o zaštiti novčarskih institucija U mjerama koje će dodatno provoditi, banke bi trebale naglasak usmjeriti na osiguranje ispravnosti i funkcionalnosti sustava koje se postiže pravilnim održavanjem i minimalnim nadogradnjama.

U Zakonu nije definirana učestalost redovnog održavanja, ali je to definirano Pravilnikom o uvjetima i načinu provedbe tehničke zaštite. Prema aktualnom Pravilniku obaveza vlasnika ili korisnika je održavati sustav najmanje jednom godišnje i to od strane tvrtke ovlaštene za poslove tehničke zaštite. To znači da svi objekti s tehničkom zaštitom, a naročito novčarske institucije, trebaju imati ugovor o održavanju s ovlaštenom tvrtkom. Zakon je više usmjeren na dokumentaciju kojom se dokazuje redovno održavanje i njime je propisano da u svakoj poslovnici treba imati original ili presliku potvrde i zapisnika o tehničkom prijemu te radne naloge kojim se dokazuje redovno servisiranje svih sustava tehničke zaštite. Kroz obavezni sigurnosni plan zaštite i sigurnosne procedure, a u sklopu mjera tehničke zašite, novčarske ustanove definiraju potrebu za održavanjem, popravcima, doradom i zamjenom uređaja i sustava, ali i način pohrane i čuvanja tehničke dokumentacije. Zakon dodatno propisuje obvezu vođenja evidencije o popisu i smještaju tehničke dokumentacije koja obuhvaća i poslove održavanja.

Da bi sustav tehničke zaštite efikasno služio kao alat u zaštiti poslovnice potrebno je osigurati njegovu potpunu funkcionalnost u svim uvjetima. Do sada važeći Zakon je definirao koje sustave treba ugraditi ovisno o kategoriji objekta, ali bez tehničkih detalja. Zakon u proceduri propisuje i zahtjeve na sustav kako bi on služio svrsi što znači da obveznici Zakona trebaju provjeriti da li postojeći sustavi zadovoljavaju tražene zahtjeve i po potrebi ih nadograditi. Kamere koje pokrivaju bitne točke (ulaze/izlaze, uplatno – isplatna mjesta, prostor diskretne blagajne i primopredaje novca pri distribuciji, te prostor u i ispred centralnog trezora) moraju imati funkciju identifikacije, što znači da moraju imati rezoluciju 330 piksela po metru. Osim toga, kamere koje pokrivaju ulaze trebaju imati široki dinamički opseg

ili WDR funkciju. Svaka poslovnica mora imati barem jedna monitor kako bi se videozapis mogao pregledati na licu mjesta, a snimač treba biti zaštićen od sabotaže i otuđenja i to njegovim smještanjem u štićenu prostoriju ili u zasebni ormaru ili u kutiju učvršćenu na podlogu.
Dojava iz sustava protuprovale/protuprepada može se slati na dojavni centar ovlaštenih zaštitara ili unutarnju zaštitarsku službu. Komunikacija s dojavnim centrom mora biti neprekidna, nadzirana i zaštićena, a ako se ne koristi nadzirana komunikacija obavezno je koristiti dva odvojena komunikacijska kanala (klasični i GSM/GPRS). Obzirom da većina banaka, svjesna nedostataka klasične telefonske linije, već duže vrijeme koristi profesionalne IP komunikatore i za poslovnice i za bankomate koji su već po aktualnom Zakonu trebali imati nadziranu komunikaciju, njima ovaj zahtjev neće donijeti ništa novo u smislu ulaganja. Dapače, neke veće banke su same, želeći još više podići nivo sigurnosti komunikacije, uz IP komunikatore uvele i GPRS rezervni način komunikacije kako bi u slučaju pada žičane komunikacije IP komunikacija bila nastavljena putem GPRS mreže. IP komunikacija za financijske institucije treba biti i u skladu s europskom normom EN50131 gdje je za banke potrebna Grade 3 oprema, a to znači nadziranu IP komunikaciju. Da bi sustavi tehničke zaštite bili funkcionalni u vrijeme incidenta potrebno je osigurati rezervni način napajanja jer je mogući način njihove sabotaže i prethodno isključivanje mrežnog napajanja. Za protuprovalu taj zahtjev nije problem jer svi sustavi protuprovale sadrže i akumulatore kao rezervni način napajanja (jedino treba voditi računa o ispravnosti akumulatora), ali treba voditi računa da se rezervno napajanje osigura i za router preko kojeg ide komunikacija. Najvažnija novost je obvezno rezervno napajanje videonadzora pri čemu treba voditi računa da ga treba osigurati i za kamere, a ne samo za snimače, jer nema smisla po nestanku napajanja osigurati napajanje snimaču ako kamere više ne funkcioniraju. To dodatno znači da se kamere moraju centralno napajati, a trebaju imati i rezervno napajanje preko UPS-a. Opet poslovnice banaka u većini slučajeva već imaju centralizirano napajanje jer su rađene po projektima u kojima se vodilo računa i o rezervnom napajanju pa će bankama izmjena biti samo UPS ili jačina UPS-a koji osigurava napajanje 30 minuta (Dončević, 2015).

Detaljnije, novim Zakonom o zaštiti novčarskih institucija naglasak je na propisivanju „optimalnih“, a ne više „minimalnih“ mjera zaštite. Zakon definira da protuprovalna vrata koja se ugrađuju u poslovnice novčarskih institucija moraju imati minimalnu razinu protuprovalnosti klase WK2 prema EN 1627. Zakon navodi da su sastavni dio protubalističke pregrade neprobojna stakla, nosive i

neprobojne konstrukcije, te vrata koja moraju zadovoljavati standarde protuprovalnosti i protubalističke otpornosti s jasno definiranom razinom koja kaže da moraju zadovoljavati minimalne uvjete otpornosti na propucavanje razine FB2/BR2.

Zakon je novim odredbama definirao da samostojeći montažni objekti moraju biti izvedeni u minimalnoj razini protubalističke zaštite FB4/BR4, a ulazna vrta moraju biti protuprovalna, minimalne klase protuprovalnosti WK4 i ne smiju imati protubalističku razinu nižu od stijene u koju su ugrađena, uključujući i spoj vrata i podne konstrukcije. Takvi objekti moraju nositi oznaku FB4/BR4/WK4.

Na uplatno isplatnim mjestima trebaju se koristiti ladice ili kase s mehaničkim ili elektroničkim zaključavanjem, a pojedini obveznici Zakona trebaju koristiti kase s vremenskom odgodom otvaranja prema EN 14450.

Prostor trezora mora imati protuprovalna vrata s mehaničkim zaključavanjem ili „suključarstvom“ i kontrolom pristupa.

4. ZAKLJUČAK

Zadatak Završnog rada obuhvaćao je opis i analizu koncepta zaštite financijske institucije te je stoga zahtijeva obilazak velikog broja poslovnica, filijala, savjetodavnih centara, 24 satnih zona, bankomata i ostalih objekata koje financijske institucije koriste na teritoriju cijele RH. Opis i analiza koncepta zaštite financijske institucije zahtijeva određena stručna znanja o implementaciji sustava tehničke zaštite i znanja legislative koja pokriva predmetno područje koje se akumulira kroz niz stručnih seminara s temama tehničke zaštite i legislative područja tehničke zaštite.

Analizom svih aspekata sigurnosti na objektima reprezentativne financijske institucije utvrđeno je da su implementirani sustavi visoko iznad prosjeka kvalitete i složenosti u odnosu na ostale sustave u RH. Samim time što se investitor nije zadovoljio minimalnim mjerama koje su propisane zakonom iskazuje se njegova ozbiljnost u provođenju što učinkovitijih mjera zaštite u svim oblicima. Kako je sama institucija po svojim financijskim rezultatima i broju klijenata također među nekoliko na samom vrhu u našoj državi jasno je da, sa financijskog aspekta gledano, ima veliku prednost pred ostalim, pa lakše ispunjava zadane uvjete. Naveden je čitav niz prijedloga, mjera i preporuka jer uvijek postoji bolja zaštita od implementirane, a pitanje je samo ostvaruje li se njome i bolji učinak odnosno opravdava li cilj sredstvo ili bi navedena poboljšanja bila samo dodatni trošak bez velikog učinka na stanje sigurnosti. Iz ovog razloga predložene su mjere koje ne iziskuju drastična ulaganja, a većinom se odnose na korištenje mrežnih tehnologija koje su danas sveprisutne te su uglavnom dio infrastrukture u kojoj je već implementiran sustav tehničke zaštite. Cijene nadogradnji su zanemarive u odnosu na one prije nekoliko godina. Zbog svega navedenog u prijedlog mjera za povećanje sigurnosti na bazi nekih od danas brzorastućih tehnologija nisu predložene kao na primjer video analitika u zaštiti perimetra i brojanju ljudi ili prepoznavanje lica i boje glasa u sustavima kontrole pristupa. Razlog je tome što te tehnologije tek dolaze, a danas implementirane ne bi dale dovoljno učinka za onu cijenu koja se traži na tržištu.

Iako su ugrađeni svi elementi koje je dosadašnji Zakon propisivao, novim Zakonom o zaštiti novčarskih institucija doći će do investicija u polju tehničke zaštite kako bi se sigurnost još više poboljšala.
Brzi razvoj novih tehnologija i pad cijena na tržištu osigurava buduću primjenu sofisticiranih alata za povećanje opće sigurnosti pa se shodno tome Koncepti zaštite redovno moraju revidirati i pomalo uvoditi nove tehnologije i sustave i to u trenutku kad oni mogu dati najbolje rezultate.

Jednakovremeno iz Završnog rada može se zaključiti da bez obzira na kompleksnost implementiranog sustave tehničke zaštite i bez obzira na uložena sredstva isti sustavi samostalno ne mogu dati zadovoljavajuće rezultate neovisno o ljudskom faktoru. Neizostavno odgovorna osoba brine se o svim komponentama sustava, kontrolira ih, servisira, sustavno razmišlja o unaprjeđenjima zaštite, kreira pravilnike, procedure, strategije, politike i ostale dokumente za cjelovito upravljanje sigurnosti jedne takve institucije.

5. POPIS LITERATURE

1. Delišimunović, D.: Suvremeni koncepti i uređaji zaštite, -Zagreb:I.T.Graf, 2002.
2. Husar, I.: Alarmni sustavi, -Zagreb: Hrvatski ceh zaštitara, 1998.
3. Ostojić, A. i dr.: Priručnik za izobrazbu čuvara i zaštitara, -Zagreb: INTER SIG, 2005.
4. Kruegle,H.: CCTV surveillance, Video practices and tehnology, -Newton: Buttereworth-Heinemann, 1995.
5. http://www.mup.hr/10.aspx
6. Novak, I.: Zaštitno-alarmni sustavi i osiguranje imovine, -Zagreb: "Osiguranje Zagreb" d.d., 1995.
7. Delišimunović, D.: Management zaštite i sigurnosti, - Zagreb: Pragmatekh, 2006.
8. Delišimunović,D.: Zaštita i sigurnost financijskih institucija, -Zagreb:Tectus d.o.o., 2001.
9. http://www.perpetuum.hr/hr/poslovno-druzenje-sigurnost-i-zastita- podataka
10. http://www.zastita.info/hr/
11. http://www.securitas.com/HR/hr-hr/Services/Tehnika-zatita/
12. http://www.eccos.com.hr/
13. http://www.alarmautomatika.com/
14. Operating manual Axessor
15. http://sigurnost.info/literatura-mainmenu-70/50-literatura/196-knjiga-management-zatite-i-sigurnosti
16. http://www.safety.hr/downloads/zbornik_radova_m&s_2009.pdf
17. Procjena ugroženosti i sigurnosni elaborat filijale Banke u Zagrebu
18. Procjena ugroženosti i sigurnosni elaborat bankomata u Zagrebu
19. http://www.alarmautomatika.com/documents/files/clipping/2015/2015-04_zastita_funkcionalnost-tehnicke-zastite-u-fokusu.pdf
20. http://www.aristokrat.hr
21. http://proalarm.hr

6. POPIS PRILOGA

Prilog 1: Suglasnost na prosudbu ugroženosti

REPUBLIKA HRVATSKA
MINISTARSTVO UNUTARNJIH POSLOVA
Broj: 511
Zagreb,

Ministarstvo unutarnjih poslova Republike Hrvatske, na temelju članka 8. stavka 6. Zakona o minimalnim mjerama zaštite u poslovanju s gotovim novcem i vrijednostima ("NN" br. 173/03 i 150/05) i članka 96. stavka 1. Zakona o općem upravnom postupku ("NN" br. 47/09), u predmetu davanja suglasnosti na prosudbu ugroženosti, po zahtjevu trgovačkog društva

d o n o s i

R J E Š E N J E

Daje se suglasnost na prosudbu ugroženosti Filijale

O b r a z l o ž e n j e

Trgovačko društvo zatražilo je izuzeće od primjene mjera zaštite, koje su za novčarske institucije I. kategorije propisane odredbama Zakona o izmjenama i dopunama Zakona o minimalnim mjerama zaštite u poslovanju s gotovim novcem i vrijednostima ("NN" br. 150/05) odnosno suglasnost na prosudbu ugroženosti Filijale

Uz podnesak su priloženi Elaborat prosudbe ugroženosti i mjera sigurnosti te Projekt izvedenog stanja sustava tehničke zaštite za navedenu filijalu, koje su izradile tvrtke koje imaju odobrenje za obavljanje djelatnosti tehničke zaštite a u kojima se predlaže da se zaštita filijale provodi već ugrađenim protuprovalnim i protuprepadnim sustavom s centraliziranom dojavom i nadzorom alarma te sustavom video nadzora s pohranjivanjem videozapisa. Ujedno ovlašteni izrađivač napominje da su u filijali, kao dodatna mjera zaštite u svrhu povećanja sigurnosti i zaštita osoba koje obavljaju poslove s gotovim novcem i vrijednostima, ugrađena sigurnosna interlocking vrata koja imaju ugrađeni video nadzor kao i sustav kontrole ulaza/izlaza u/iz filijale uz mogućnost zaključavanja interlocking vrata i to na način koji ne ugrožava djelatnike i stranke filijale a čije su stijene izrađene od neprobojnog stakla koje pruža najmanju razinu neprobojne zaštite BR3/S odnosno koje pruža zaštitu od ispaljenog projektila cal. 0,357 Magnum. Isto tako u filijali su u uporabi sustavi kontrole pristupa dok se na uplatno/isplatnim mjestima koriste blagajne s vremenskom odgodom.

Ovlaštena tvrtka koja je izradila prosudbu ugroženosti razvrstala je filijalu na temelju prosudbe ugroženosti u III. kategoriju iz Pravilnika o uvjetima i načinu provedbe tehničke zaštite ("NN" br: 198/03.) te smatra da izvedene mjere tehničke zaštite u i oko filijale predstavljaju potrebnu razinu zaštite te da nije potrebno uvoditi tjelesnu zaštitu u sam prostor filijale tijekom cjelokupnog radnog vremena kao ni radni prostor zaposlenika pregrađivati neprobojnim pregradama od prostora dostupnog strankama.

U postupku provedenom povodom zahtjeva izvršen je uvid u priloženu dokumentaciju a od strane nadležnog inspektora Ministarstva unutarnjih poslova je, dana
godine, obavljen inspekcijski nadzor poslovnog prostora kojim je utvrđeno da su u filijali izvedeni protuprovalni i protuprepadni sustav s centraliziranom dojavom i nadzorom alarma te sustav video nadzora s pohranjivanjem videozapisa. Nadzorom je utvrđeno da su kao dodatne mjere zaštite u filijali ugrađena sigurnosna interlocking vrata koja imaju ugrađeni video nadzor kao

Prilog 2: zapisnik o tehničkom prijemu

_____
(NAZIV I SJEDIŠTE TRGOVAČKOG DRUŠTVA ILI OBRTNIKA)

Na temelju članka 22. stavka 3. Pravilnika o uvjetima i načinu provedbe tehničke zaštite ("Narodne novine", br. 198/03.) sastavlja se

Z A P I S N I K

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

_____
(broj Ugovora)

sklopljenog sa:

_____.
(naziv i sjedište pravne osobe ili adresa obrtnika)

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

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

U _____
(mjesto i datum)

Za naručitelja: Za izvođača:

._____ _____
(potpis naručitelja) (potpis ovlaštenog predstavnika izvođača)

Prilog 3: potvrda o izvedbi sukladno sa Pravilnikom o uvjetima i načinu provedbe tehničke zaštite

_____
(NAZIV I SJEDIŠTE TRGOVAČKOG DRUŠTVA ILI OBRTNIKA)

Na temelju članka 22. stavka 4. Pravilnika o uvjetima i načinu provedbe tehničke zaštite ("Narodne novine", br. 198/2003.) izdaje se

P O T V R D A

kojom se potvrđuje da je izvedba sustava tehničke zaštite, prema Ugovoru broj: _____,
(broj Ugovora)

sklopljenog s naručiteljem posla _____, koji je u svojstvu
(naziv pravne ili fizičke osobe)

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

obavljena sukladno odredbama uvodno navedenog Pravilnika.

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

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

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

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