ORGANIZACIJA SIGURNOSTI U FINANCIJSKIM INSTITUCIJAMA

Špoljar, Krešimir

Master's thesis / Specijalistički diplomski stručni

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Karlovac University of Applied Sciences / Veleučilište u Karlovcu**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:128:430166

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Krešimir Špoljar

ORGANIZACIJA SIGURNOSTI U FINANCIJSKIM INSTITUCIJAMA

ZAVRŠNI RAD

Karlovac 2021.

Karlovac University of Applied Sciences
Safety and Protection Department

Professional graduate study of Safety and Protection

Krešimir Špoljar

SECURITY ORGANIZATION IN FINANCIAL INTITUTIONS

FINAL PAPER

Karlovac 2021.

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Krešimir Špoljar

ORGANIZACIJA SIGURNOSTI U FINANCIJSKIM INSTITUCIJAMA

ZAVRŠNI RAD

MENTOR:

Davor Kalem, struč. spec. krim.

Karlovac 2021.

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Specijalistički studij: Sigurnosti i zaštite

Usmjerenje: Zaštita na radu Karlovac, 2021.

ZADATAK ZAVRŠNOG RADA

Student: Krešimir Špoljar Matični broj: 0248019424

Naslov: Organizacija sigurnosti u financijskim institucijama

1. Opisati razvoj financijskih institucija
2. Definirati zakonske odredbe u vezi financijskih institucija
3. Pojasniti vrste financijskih institucija
4. Analizirati vrste ugrožavanja financijskih institucija
5. Opisati mjere zaštite financijskih institucija
6. Prikazati slučajeve ugrožavanja financijskih institucija
7. Opisati prijedloge mjera poboljšanja zaštite financijskih institucija

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
svibanj 2021.	listopad 2021.	2. 12. 2021.

Mentor: Predsjednik Ispitnog povjerenstva:

Davor Kalem, predavač Marko Ožura, viši predavač

PREDGOVOR

Kroz svoje cjelokupno studiranje na Veleučilištu u Karlovcu, unaprijedio sam svoje stručno znanje iz područja zaštite na radu. Kroz četiri godine rada na poslovima struke teoretski dio svakodnevno primjenjujem u praktičnom radu na poslovima zaštite na radu. Temu završnog rada iz kolegija tjelesne zaštite izabrao sam kako bih proširio svoje znanje iz tog područja te u budućnosti pokušati primijeniti naučeno znanje na poslovima koje obavljam.

Ovim putem želim zahvaliti svojim roditeljima koji su me gurali i pomagali u mom studiranju, pogotovo na stručnom diplomskom studiju, a kasnije i podrškom na specijalističkom dijelu.

Za kraj, ne smijem zaboraviti zahvaliti mentoru Davoru Kalemu na ukazanoj prilici za završni rad, velikoj pomoći i uputama kroz pisanje rada.

SAŽETAK

Pravnim regulativama i aktima RH definirani su temelji zaštite novčarskih institucija. Tjelesna i tehnička zaštita financijskih institucija i njihovih objekata je unaprijed definirana, prema kategorizaciji štićenih objekata. Vrsta zaštite, provedba zaštite i smjernice su regulirane pravnim obvezama, bilo da se radi o objektima centralnih banaka, poslovnica, bankomatima ili zaštiti vrijednosti prilikom transporta. Financijske institucije, pogotovo manji objekti s nižim stupnjem zaštite su često na meti razbojnika. Baš zbog tog nižeg stupnja zaštite, te zahtjeva za složenost zaštite tehničkim i tjelesnim metodama zaštite, razbojnicima je lakše izvršiti pljačku s manjim mogućim posljedicama i gotovo nikakvom potrebom za razradu plana pljačke. Nadalje je bitno spomenuti da su sami oblici napada na financijske institucije promijenili način na koji se danas pljačka. *Cyber* napadi na financijske institucije postali su učestali unazad nekoliko godina, s velikim posljedicama za korisnike, a naročito za financijske institucije i njihovo poslovanje. Tjelesna i tehnička zaštita je obaveza kada govorimo o zaštiti financijskih objekata od fizičkih napada, a cyber sigurnost je obaveza kada govorimo o sve učestalijim hakerskim napadima.

Ključne riječi: financijske institucije; tjelesna zaštita; tehnička zaštita; *cyber* zaštita; zaštita osobnih podataka; napadi na financijske institucije

SUMMARY

Legal regulations and acts of the Republic of Croatia define the foundations for the protection of financial institutions. Physical and technical protection of financial institutions and their facilities is defined in advance, according to the categorization of protected facilities. The type of protection, the implementation of protection and the guidelines are regulated by legal obligations, whether it is the facilities of central banks, branches, ATMs or the protection of value during transport. Financial institutions, especially smaller facilities with a lower level of protection, are often targeted by bandits. Precisely because of this lower level of protection, and the requirements for the complexity of protection by technical and physical methods of protection, it is easier for robbers to commit a robbery with minor possible consequences and almost no need to develop a robbery plan. It is further important to mention that the very forms of attacks on financial institutions have changed the way robbery is done today. Cyber attacks on financial institutions have become more frequent over the past few years, with major consequences for users, and especially for financial institutions and their businesses. Physical and technical protection is an obligation when we talk about protecting financial facilities from physical attacks, and cyber security is an obligation when we talk about the increasingly frequent hacker attacks.

Keywords: financial institutions; physical protection; technical protection; cyber protection; protection of personal data; attacks on financial institutions

SADRŽAJ

1. UVOD

Živimo u 21. stoljeću, doba u kojoj je sigurnost na najvišem nivou ikada, ali treba napomenuti i da je sigurnost pojedinca, njegove materijalne i nematerijalne imovine, sigurnost države, ustanova i nacije u nikada većoj opasnosti od zadiranja u osobnu sigurnost i njezinog narušavanja. U vremenu u kojem živimo, nikada nije lakše izgubiti sigurnost. Za početak, treba se voditi činjenicom da se na našem dlanu (pametnom telefonu, tabletu, pametnom uređaju…) nalazi „cijeli svijet“ informacija, kako o nama, tako i o našim osobnim podatcima, bankovnim računima… Te iste podatke, netko tko dobro rukuje računalima i računalnim programima, može iskoristiti radi osobne zarade, krađe novca s bankovnog računa, krađu identiteta, moguće ucjene i slično.

Međutim, ako gledamo bankarsku sigurnost i sigurnost ostalih financijskih institucija koje se obrađuju u ovoj temi, sigurnost je na visokoj razini. No budući da je tehnologija preskočila ne jednu, nego tri stepenice, tako se i tehnička zaštita objekata podigla na jednu zavidnu razinu i omogućila da se uspješno i pravovremeno isti objekti zaštite, te da se pravovremeno djeluje bez posljedica. Današnja tehnologija omogućuje fizičkoj osobi da za nekoliko stotina kuna postavi sustav videonadzora u vlastite stambene objekte.

Ukoliko se vratimo na financijske institucije, današnja situacija je takva da najveću prijetnju predstavljaju *cyber* napadi na bankovne račune i programske sustave banaka. S obzirom koliko je sustav tehničke zaštite institucija napredovao, velike pljačke koje možemo gledati u filmovima i televizijskim serijama manje su vjerojatne. Svakako iste ne treba isključiti, da u trenutku neželjenih događaja, sustav može djelovati bez ljudskih i materijalnih posljedica.

Manji objekti u kojima se obavljaju gotovinske transakcije, kasina, poštanski uredi i slični objekti, budući da kao takvi pripadaju i manjoj kategoriji zaštite, predstavljaju potencijalno lakši „plijen“ za razbojnika.

Kako primjena novih tehnologija nudi velik broj mogućnosti, tržište se iz dana u dan sve više i više širi, cijene uređaja zaštite padaju, a tehnologija i mogućnosti tih uređaja će nastaviti uzlaznom putanjom. Nove ideje inženjerskih timova će povećavati praktičnost i uporabu, integrirati jedne sustave u druge, međusobno ih povezivati i

prilagođavati ih kako hardverski, tako i softverski. Programska rješenja i antivirusni sustavi zaštite financijskih institucija se ubrzano ažuriraju, kako bi se pružila maksimalna zaštita financijskim institucijama i njihovim korisnicima.

2. RAZVOJ FINANCIJSKIH INSTITUCIJA

Novac je vrijednosna valuta koja služi za trgovanje i razmjenu robom, odnosno vrijednost kojom se kupuje duga protuvrijednost koja može biti bilo što. Novac upotrebljavamo za kupovinu potrepština ili za otplatu dugova. Prije same pojave novca, bila je na snazi razmjena dobara, u kojoj se roba X razmjenjivala za robu Y, poznatije kao pojam trampa. Stočar je stoku davao za brašno, ratar je kukuruz davao za meso, stolar svoje proizvode od drveta za metal itd. Međutim, događale su se situacije kada, zbog ponude i potražnje, seljak nije mogao svoju robu zamijeniti za drugu zbog zasićenosti zaliha. Tada se pojavila potreba za univerzalnim rješenjem kojim bi jedna univerzalna roba mogla služiti za kupovinu i prodaju robe za određenu vrijednost i s tom vrijednosti je seljak mogao kupiti željenu robu u propisanoj količini koja bi zadovoljila njegove potrebe. Oko 1000 godina pr. Kr. u Aziji, točnije Kini, novac je imao nešto drugačiji oblik od kovanice, koji je imao svoju vrijednost. Legura tih vrijednosnih predmeta bila je od bronce ili bakra, a ovisno o području gospodarske djelatnosti imala je svoj oblik, odnosno predstavljala alat ili oruđe te djelatnosti. Primjerice, na područjima regija koje su bile poznate po kovačkim zanatima, novac je bio izrađen u obliku noža, a regije poznate po poljoprivredi, imale su novac u obliku lopate i slično. Svaki taj vrijednosni predmet na sebi je imao ugraviranu vrijednost, ovisno o masi ili veličini. [1]

Prvi službeni kovani novac, izdan je u 7. stoljeću pr. Kr. na području Lidijaca u Maloj Aziji, a kasnije se taj „trend“ proširio na Mediteran. Čak se smatra da su 500 godina ranije kovanice bile prisutne u Indiji i Kini. Kovanice su na sebi imale utisnut državni žig iza kojeg je stajala država i polagala pravo na kovanje. Kovanice su bile ručno izrađene od mješavine legura srebra i zlata, a na njima su bili otisnuti razni simboli bogova, raznih vladara ili dinastija, mitoloških bića, životinja itd. Kasnije svako carstvo kuje i izrađuje svoje verzije kovanica koje kontrolira isto. Primjerice, Rimsko carstvo izrađuje svoj bakreni novac (*aes*) i njegove verzije koje imaju različite vrijednosti: *uncia* (1/12 *aesa*), *semis* (6 *uncia*), *triens* (4 *uncia*)… Kasnije, u 3. stoljeću pr. Kr. pojavljuje se srebrni novac *denaruis* i krajem Republike zlatni novac *aureus*. Nakon raspada Rimskog Carstva germanski narodi preuzimaju rimski novac i njegovo kovanje. [2]

Međutim, problem kovanog novca bio je taj što je veća količina istog bila problem za transport zbog velike mase. Kineski vladari su u ono vrijeme uveli vrijednosne papirnate potvrde za trgovinu kako bi zadržali kovanice u svojim riznicama. Tako su ljudi s tim potvrdama kasnije mogli kupovati zlato ili srebro, a kasnije ga ponovno zamijeniti u kovanice. Porastom globalne trgovine i različitih novčanih valuta te njezinih vrijednosti, postavilo se pitanje uvođenja univerzalne i jedinstvene vrijednosti koja će pokriti svaku valutu. Tako je zlato izabrano za opravdavanje vrijednosti papirnatih novčanica, te je svaka novčanica morala imati zlatnu zalihu za njezinu vrijednost. [3]

Godine 1821. Bank of England prva uvodi zlatni standard, koja je svojim autoritetom jamčila da će sva vrijednost zlata biti isplaćena u papirnatim novčanicama. Time su globalne cijene stabilizirane i novčane valute su imale svoju ustaljenu i zajamčenu vrijednost. Nastankom Prvog svjetskog rata dolazi do globalnih kriza, inflacije, izdavanja novca bez pokrića, što kasnije dovodi do kraja ere zlatnog standarda. [1]

Tijekom osamdesetih i devedesetih godina XX. tolјeća bankarska industrija doživjela je veliku krizu, ponajprije zbog lošeg poslovanja banaka, lošom raspodjelom depozita i daljnjim zatrpavanjem u dugove. Nakon te financijske krize, bankarski sustav se počinje uzdizati, a bankarske tvrtke se udružuju u veće institucije i osnivaju velike globalne bankarske sustave. Predviđalo se da će se ubrzo sve bankarske tvrtke udružiti u nekoliko glavnih i tako kontrolirati globalno poslovanje i sav globalni dug. Zadnja bankarska kriza dogodila se 2017. godine, kada su se banke međusobno počele zaduživati i gomilati dugove, a rezultirala je smanjenjem banaka i povećanjem internet bankarstva. No valja napomenuti da te banke nisu nestale nego su se povezale u veće korporacije. [4]

Modernizacijom i tehnologijom papirnati novac se polako izbacuje iz opticaja, a uvelike se svodi na online transakcije novca i kupovinu, s računa na račun. Velike količine novca mogu se prebaciti u nekoliko sekundi na globalnoj razini. Digitalizacijom su se otvorila vrata nekim novim valutama. Kriptovalute su novi trend u transakcijama i razmjeni vrijednosti. Vrlo su sličnih karakteristika kao i novac, ali ne posjeduju fiksnu vrijednost. Ta vrijednost često se mijenja nekoliko puta dnevno. Teško ih se krivotvori, vrlo brzo se mogu razmijeniti između osoba koje s njima trguju, te su u ograničenim količinama koji su u opticaju. Međutim, vlade država još uvijek nisu prihvatile porez u

kriptovalutama te se zbog toga još uvijek vode kao sredstvo razmjene. Valja napomenuti da kriptovalute nemaju centralnu banku koja ih kontrolira. [3]

3. PRAVNE REGULATIVE, ZAKONI I PROPISI

Budući da se radi o temi koja zahtjeva usuglašenost sa svim važećim pravnim propisima i normama Republike Hrvatske te međunarodnim propisima, prilikom čije se izrade nailazilo na veliki broj istih, navest će se najvažnije za koje se smatra da su neophodni za postavljanje sigurnosno-zaštitnog koncepta financijskih institucija. Zakoni koji su propisani osnova su za temelj postavljanja sigurnosti u objektima, a pravilnici su ti koji propisuju detaljne obaveze i pravila za pojedine segmente tehničkih ili tjelesnih mjera zaštite.

Ugrožavanje novčarskih institucija i objekata za novčane transakcije predstavlja kazneno djelo imovinskog delikta (Glava XXIII. Kaznenog zakona Republike Hrvatske). Imovinski delikt je kazneno djelo u kojem počinitelj drugome oduzme tuđu pokretnu stvar s namjerom da istu protupravno prisvoji. [5]

Kroz ovaj rad proći će se kroz najvažnije zakone, propise i regulative:

Zakoni:

- Kazneni zakon Republike Hrvatske[1]
- Zakon o zaštiti novčarskih institucija[2]
- Zakon o privatnoj zaštiti[3]
- Zakon o gradnji[4]
- Zakon o prostornom uređenju i gradnji[5]
- Zakon o informacijskoj sigurnosti[6]
- Zakon o zaštiti tajnosti podataka[7]

[1] Kazneni zakon Republike hrvatske (Narodne novine, 84/2021)
[2] Zakon o zaštiti novčarskih institucija (Narodne novine, 56/15, 46/21)
[3] Zakon o privatnoj zaštiti (Narodne novine, 16/20)
[4] Zakon o gradnji (Narodne novine, 153/13, 20/17, 39/19, 125/19)
[5] Zakon o prostornom uređenju i gradnji (Narodne novine, 153/13, 65/17, 114/18, 39/19, 98/19)
[6] Zakon o informacijskoj sigurnosti (Narodne novine, 79/07)
[7] Zakon o zaštiti tajnosti podataka, (Narodne novine, 108/96) (Ovaj zakon je stupio na snagu 31.12.1996., a prestao važiti 06.08.2007. stupanjem na snagu Zakona o tajnosti podataka, osim odredaba glave 8. i 9.)

- Zakon o tajnosti podataka[8]
- Zakon o sigurnosnim provjerama[9]
- Zakon o kritičnim infrastrukturama[10]

Pravilnici:

- Pravilnik o uvjetima i načinu provedbe tehničke zaštite[11]
- Pravilnik o uvjetima i načinu provedbe tjelesne zaštite[12]
- Pravilnik o prostornim i tehničkim uvjetima koje mora ispunjavati prostor u kojem se obavlja djelatnost privatne zaštite[13]
- Pravilnik o prostornim i tehničkim uvjetima za priređivanje igara na sreću u casinima[14]

3.1. Kaznena djela

Kaznena djela imovinskih delikata Glave XXIII. Kaznenog zakona Republike Hrvatske možemo podijeliti na:

1. Krađa – najčešći oblik imovinskog delikta, od amaterskim maloljetničkih krađa u malim prodavaonicama do profesionalnih kradljivaca s već dobro uhodanim zanatom. Iskusni kradljivci većinom djeluju u grupama, u kojima jedna ili više osoba (počinitelj/a) napravi distrakciju (pojam skretanja pozornosti) žrtvi, okupira njezinu pažnju dok drugi počinitelj izvrši otuđenje. Ovdje možemo navesti jedan od najčešćih primjera, krađa u trgovinama, gdje jedna osoba iz grupe odvraća pažnju prodavača tako da ga zapriča dok ostatak grupe (jedna ili više osoba) uzima predmete, robu itd. [10]

[8] Zakon o tajnosti podataka (Narodne novine, 86/12)
[9] Zakon o sigurnosnim provjerama (Narodne novine, 85/08, 86/12)
[10] Zakon o kritičnim infrastrukturama (Narodne novine, 56/13)
[11] Pravilnik o uvjetima i načinu provedbe tehničke zaštite, Narodne novine, 198/2003)
[12] Pravilnik o uvjetima i načinu provedbe tjelesne zaštite, Narodne novine, 45/2005)
[13] Pravilnik o prostornim i tehničkim uvjetima koje mora ispunjavati prostor u kojem se obavlja djelatnost privatne zaštite, Narodne novine, 29/2005)
[14] Pravilnik o prostornim i tehničkim uvjetima za priređivanje igara na sreću u casinima, Narodne novine, 38/10 (Pravilnik o izmjenama i dopunama NN36/20)

2. Teška krađa - ona se od obične krađe razlikuje u tome na koji je način počinjena i pod kojim okolnostima, te prema vrijednosti predmeta krađe. Teške krađe[15] su krađe koje su počinjene:

- obijanjem, provaljivanjem ili savladavanjem većih prepreka
- na osobito opasan ili drzak način
- iskorištavanjem stanja prouzročeno višom silom
- iskorištavanjem bespomoćnosti druge osobe
- ako je ukradena borbena oprema koja služi u svrhu obrane
- ako je ukraden predmet služi u vjerske svrhe
- ako je ukradeno kulturno dobro
- ako je počinitelj pri sebi imao oružje ili opasan predmet
- ako je službena osoba obavila krađu pri službenoj dužnosti. [5]

Tešku krađu možemo objasniti na primjeru krađe i nezakonitog trgovanja motornih vozila, kojima se bave organizirane kriminalne skupine, poznatije pod nazivom automafija. Mjesta krađe najčešće su slabo osvjetljeni parkinzi i manje uočljiva mjesta na kojima razbojnik može lakše izvršavati radnje potrebne za otvaranje automobila. Najčešći oblici krađa su otvaranje ili razbijanje prozorskih stakala, obijanje brava na prtljažniku, a na novijim vozilima sa centralnim zaključavanjem se razbojnici koriste informatičkim uređajima za presretanje signala od ključa automobila. Prema podacima Eurostata, u razdoblju od 2015. do 2017. godine, prosjek godišnjih krađa bio je 697.000 automobila. [11]

3. Razbojništvo – kazneno djelo koje je počinjeno uporabom sile ili pod prijetnjom da će izravno napasti život ili tijelo neke osobe, s ciljem protupravnog prisvajanja tuđe pokretne stvari. Kazna za ovakvu vrstu kriminalnog djela je zatvorska kazna od jedne do deset godina. [5]

Pod uporabu sile podrazumijevamo apsolutnu i psihičku silu. Apsolutna sila je uporaba fizičke snage ili sredstava kako bi se žrtva fizički onesposobila. Uporaba psihičke sile

[15] Prema članku 229. Kaznenog zakona RH (Narodne novine, 84/21)

podrazumijeva da je žrtva fizički sposobna pružiti otpor, ali je zbog psihološkog stanja onemogućena pružiti otpor. [12]

4. Razbojnička krađa – kazneno djelo u kojem je počinitelj prilikom zatjecanja u krađi uporabio silu protiv osobe ili prijetio osobi da će napasti njezin život ili zdravlje, s ciljem da ukradenu stvar zadrži. [5]

Razlika između razbojništva i razbojničke krađe je ta što u razbojništvu uporaba sile dolazi prije otuđivanja predmeta, a kod razbojničke krađe sila dolazi nakon otuđivanja predmeta. [12]

5. Iznuda – kazneno djelo s ciljem da sebi ili drugom protupravno pribavi imovinsku korist uporabom sile ili pod prijetnjom, na štetu svoje ili tuđe imovine. [5]

Najbolji primjer ovog kaznenog djela je prisilna zaštita ili tzv. „reket“. Reketarenje je poznati urbani sleng kojim gangsteri poduzetnicima naplaćuju svoju zaštitu. Poznati primjeri reketa datiraju još u početku 19. stoljeća, u doba talijanske mafije (*Cosa Nostra*), kada su na svome području u New Yorku, pod izgovorom zaštite lokala i posla, poduzetnicima naplaćivali velike iznose. U protivnom, ukoliko bi poduzetnici odbili njihove usluge „zaštite“, suočavali su se s uništavanjem lokala, poslovanja, fizičkim zlostavljanjima, prijetnjama i često smrću.

Jedna od najpoznatijih oružanih pljački dogodila se 1987. godine u Engleskoj, točnije u Knightsbridge-u, a objekt pljačke bio je Knightsbridge sigurnosni depozit. Napadač Valerio Viccei bio je vođa napada, koji se godinu dana prije doselio u Englesku iz rodne Italije, u kojoj je ranije izveo preko 50 oružanih pljački. Pljačku je izveo uz pomoć Parveza Latifa i nekolicine pomagača u pljački. Dana 12.07.1987. Viccei i Latifa su ušli u centar za sigurnosni depozit Knightsbridge i tražili najam sefa za sigurnosni depozit. Kada su pušteni u trezor, obojica su izvukli pištolje, onesposobili zaštitare i upravitelja te su na vrata centra stavili znak da je centar zatvoren. Kada su to napravili, pustili su svoje pomagače unutar centra. Razbojnici su otvarali sefove unutar trezora i ukrali oko 60 milijuna funti, što je prema tadašnjem tečaju iznosilo preko 98 milijuna američkih dolara. Pljačka je odrađena sat vremena prije druge smjene, kada su napadači već pobjegli s mjesta zločina. Tek dolaskom druge smjene je uočena i prijavljena pljačka. U forenzičkoj obradi pronađen je otisak Valeria Vicceia, koji je poslije pljačke pobjegao

u Latinsku Ameriku, a uhvaćen je u organiziranoj akciji kada je boravio u Engleskoj. Većina suučesnika pljačke je uhićena. [28]

Oružana pljačka Dunbar dogodila se 1997. godine kada je grupa pljačkaša otuđila oko 19 milijuna američkih dolara u gotovini, što se smatra najvećom pljačkom gotovinskog novca na svijetu. Pljačka se dogodila 12.09.1997. u skladištu oklopnih vozila Dunbar u Los Angelesu u kojima je bio novac namijenjen za bankomate. Alen Pace, koji je radio u Dunbaru kao inspektor za sigurnost, fotografirao je skladište, proučavao ga i smišljao plan kojim bi mogao ukrasti gotovinu. Proučavao je sigurnost cjelokupnog sustava i tražio njegove greške i slabosti, te ih bilježio, i u konačnici ga realizirao uz pomoć pet pomagača. Budući da je bio inspektor za sigurnost, imao je pristup sigurnosnim kamerama i sustavu. Jednom kada je ušao u sustav, rasporedio je kamere tako da iste ne vide pljačkaše, kako bi mogli pobjeći. U sobi za pauze, dočekivali su zaštitare i jednog po jednog su ih onesposobljavali. Pace je namjerno organizirao pljačku u vrijeme kada je znao da je glavni trezor otvoren zbog transfera novca, znao je točno u kojim se vrećama nalaze koje količine novca i koje su bile najvrijednije, te su otuđili. Pljačkaši su ukrali oko 19 miliona američkih dolara, koje su utovarili u transportno vozilo i udaljili se od mjesta krađa, a po završetku krađe Pace je sa sobom uzeo snimke sigurnosnih kamera.

Kako je Pace nedavno prije pljačke bio otpušten iz tvrtke Dunbar, policija ga je sumnjičila za pljačku, budući da su svi dokazi upućivali da je to bio unutarnji posao, ali nisu mogli nikoga optužiti jer nisu imali čvrstih dokaza. Pljačkaši, kako bi oprali novac, unajmili su financijskog stručnjaka da prikrije njihov novac, transakcije i isplate. Pace je svoj novac prikrio tako da je na drugog čovjeka kupovao nekretnine koje nisu bile povezane s njegovim imenom. Isti su princip primijenili i drugi pljačkaši i tako dio novca prali preko nekretnina.

Policija je uspjela doći do čvrstih dokaza kada je jedan od pljačkaša platio posredniku za nekretnine s velikom količinom gotovinskog novca, među kojima su bile označene markirane novčanice. Policija je na kraju uspjela identificirati jednog od pljačkaša koji je iznajmio kamiončić kojim su pljačkaši pobjegli s novcem iz skladišta oklopljenih vozila, a potom je pljačkaš priznao sve i dao policiji imena ostalih sudionika pljačke. [29]

Godine 2015. dogodila se oružana pljačka Istarske kreditne banke u Višnjanu. Pljačka se dogodila u jutarnjim satima, nedugo nakon otvaranja banke. Dvojica nepoznatih počinitelja naoružani su ušli u banku i zaprijetili djelatnici da joj odmah preda novac. Pod prijetnjama i u strahu za vlastitu sigurnost, predala im je traženi novac, a pljačkaši su pobjegli u nepoznatom smjeru. To je bila druga pljačka iste banke u nešto manje od dvije godine. Naime, 2013. godine u istoj banci je usred pljačke ustrijeljen zaštitar vatrenim oružjem. Napadač je u popodnevnim satima utrčao u banku i pucao na zaštitara. Pod prijetnjom je otuđio novac i pobjegao u smjeru obližnjeg trga, gdje je nespretno izgubio nekoliko snopova novčanica. U bijegu je pokušao ukrasti auto od jedne prolaznice koja je u uspjela pobjeći u vozilu. Međutim, nakon toga došao je do drugog vozila, oružjem zaprijetio vozaču i ukrao automobil, koji je policija isti dan pronašla u okolici Pazina. [31]

3.2. Kategorizacija financijskih institucija

Financijske institucije[16] su podijeljene po sljedećim primjenama mjera zaštite: [6]

1. Objekti Hrvatske narodne banke štite se:
   - Protuprepadnim i protuprovalnim sustavima za centralnu dojavu i nadzor alarma, neprekidnim videonadzorom s pohranom, sustavima kontrole pristupa s propisanim procedurama.
   - Pohrana vrijednosti i novca u trezore, centralne ili s vremenskom odgodom otvaranja. Isti trezori se također štite s istim mjerama zaštite, prethodno navedeni. Na kraju je obavezna naoružana tjelesna zaštita objekta.

2. Centralni objekt Hrvatskog novčarskog zavoda štiti se mjerama objekta kategorije 1., a prodajna mjesta zavoda se štite sljedećim mjerama:
   - protuprepadnim i protuprovalnim sustavima za centralnu dojavu i nadzor alarma, neprekidnim videonadzorom s pohranom.
   - Vrijednosti se pohranjuju u čvrste prostore sa staklenim elementima s mehaničkim otvaranjem, a novac u ladice ili kase s mehaničkim ili

[16] Članak 7. Zakona o zaštiti novčarskih institucija (Narodne novine, 56/15)

elektroničkim otvaranjem. Novac koji prelazi maksimalni limit, odlaže se u mehaničke kase.

3. Poslovnice FINA – e štite se:
   - protuprepadnim i protuprovalnim sustavima za centralnu dojavu i nadzor alarma, neprekidnim videonadzorom s pohranom, sustavima kontrole pristupa s propisanim procedurama.
   - Manipulativni novac pohranjuje se u kase ili ladice s vremenskom odgodom. Pohrana novca koji prelazi dnevni limit, odlaže se u centralne trezore, trezore, neprobojne prostore s protuprovalnim ili nekom drugom vrstom neprobojnih sefova s mehaničkim otvaranjem ili vremenskom odgodom. Ove prostore štitimo protuprovalnim i protuprepadnim sustavima, te s video nadzorom s pohranom. Trezori su osigurani kontrolom pristupa, a centralni trezor mehaničkom zaštitom predprostora s čeličnim vratima.
   - Dnevno-noćni trezori štićeni su protuprovalnim sustavima s dojavom i neprekidnim videonadzorom. Sustav za dojavu spojen je na CDS zaštitarske tvrtke. Svi depozitni sefovi moraju imati certifikat EN 1143-2[17]. [40] Te obaveznom naoružanom tjelesnom zaštitom.[18] [41]

4. Poslovnice banaka i štednih banaka s bankomatima, dnevno-noćnim trezorima, depozitnim spremnicima i bankomati drugih pravnih osoba štite se:
   - protuprepadnim i protuprovalnim sustavima za centralnu dojavu i nadzor alarma, neprekidnim videonadzorom s pohranom, sustavima kontrole pristupa s propisanim procedurama, tjelesnom zaštitom, pohrana manipulativnog novca u kase ili ladice s vremenskom odgodom otvaranja.

[17] Certifikat EN 1143-2 jedinica za sigurnu pohranu je europski standard koji utvrđuje zahtjeve i metode ispitivanja depozitnih sistema, te ih klasificira prema njihovoj otpornosti na provale.

[18] 5. rujna 2005. godine izvršena je pljačka na poslovnicu Fine u Zvonimirovoj u Zagrebu. Pljačka je ishodila s ubojstvom dvojice zaštitara (jedan je na mjestu ostao mrtav, drugi je idući dan preminuo od posljedica ranjavanja) i otuđenjem novca u vrijednosti od 2.019.025,00kn. U pljački je sudjelovalo troje razbojnika, od kojih su dvojica bili naoružani automatskom puškom tipa kalašnjikov (M70) i pištoljem, a treći sudionik je čekao u automobilu spremnim za bijeg. Zaštitari su ubijeni automatskom puškom. Zaštitari su bili naoružani, ali nisu nosili pancirke.

- Pohrana novca iznad limita, pohranjuje se u centralne trezore ili čvrste prostore s protuprovalnim vratima, sefove s mehaničkim otvaranjem ili vremenskom odgodom, ako se nalaze izvan centralnih trezora.

4.1. Centralni trezori, trezori, neprobojni prostori i prostorije štite se: protuprovalnom i protuprepadnom zaštitom, videonadzorom s pohranom, kontrolom pristupa, a centralni trezor, dodatnim predprostorom s mehaničkom zaštitom s čeličnim vratima.

4.2. Uplatno isplatna mjesta, kojima su omogućene transakcije iz vozila – protubalističkim pregradama, glasovnom komunikacijom i transfer ladicama.

4.3. Interni bankomati – protuprovalni sustav s detekcijom otvaranja vrata, koji detektira svaki nasilni pokušaj otvaranja vrata na CDS zaštitarske tvrtke. Video nadzor s pohranom je postavljen tako da osim korisničkog dijela, snima i pozadinu bankomata, te u skladu s procjenom ugroženosti i ostatak prostora. Sustav elektrokemijske zaštite u slučaju nasilnog otvaranja označava i uništava novčanice. Sukladno propisima privatne zaštite, svaka banka provodi procjenu ugroženosti.

4.4. Eksterni bankomati – štite se sustavima elektrokemijske zaštite, gdje se svaki nasilni pokušaj otvaranja detektira, te označuje i uništava novčanice, aktivira se alarm koji dojavljuje CDS-u zaštitarske tvrtke. Obavezan videonadzor s neprekidnim snimanjem i pohranom podataka, koja se pohranjuje ili na snimač unutar bankomata ili unutar prostorije u kojoj se nalazi bankomat, s protusabotažnim metalnim kućištem.

4.5. Novi eksterni bankomat – koji se postavlja ili zamjenjuje stari, mora prije postavljanja se opremiti sustavom elektrokemijske zaštite.

4.6. Interni i eksterni bankomati – koji imaju komunikaciju s bankomatima CDS-om, moraju biti rađeni po EN 1143-1 protuprovalnom certifikatu.

4.7. Dnevno noćni bankomati – štite se protuprovalnim sustavom protiv nasilnog otvaranja gdje pokušaje povale dojavljuje na CDS i obaveznim neprekidnim videonadzorom s pohranom. Svi sefovi moraju imati protuprovalni certifikat EN 1143-2.

4.8. Sigurnosno depozitni spremnici – štite se kombiniranom zaštitom.

5. Stambene štedionice:
   - protuprepadnim i protuprovalnim sustavima za CD i nadzor alarma, neprekidnim videonadzorom s pohranom.
   - Manipulativni novac pohranjuje se u kase ili ladice s vremenskim otvaranjem.
6. Poštanski uredi:

   6.1. Mali poštanski uredi s prosječnim dnevnim prometom do 30.000kn štite se - protuprepadnim i protuprovalnim sustavima za CD i nadzor alarma, neprekidnim videonadzorom s pohranom. Manipulativni novac pohranjuje se u kase ili ladice s mehaničkim ili elektronskim otvaranjem.

   6.2. Srednji poštanski ured s prosječnim dnevnim prometom od 30.000 do 150.000 kuna štite se - protuprepadnim i protuprovalnim sustavima za CD i nadzor alarma, neprekidnim videonadzorom s pohranom. Manipulativni novac pohranjuje se u kase ili ladice s vremenskom odgodom otvaranja.

   6.3. Veliki poštanski ured s prosječnim dnevnim prometom iznad 150.000 kuna štite se - protuprepadnim i protuprovalnim sustavima za CD i nadzor alarma, neprekidnim videonadzorom s pohranom. Manipulativni novac pohranjuje se u kase ili ladice s vremenskom odgodom otvaranja. Prostore štite naoružani zaštitari.

   6.4. Pokretni poštanski uredi – opremljeni su videonadzorom u objektu, opremljeni minimalno dvjema kamerama s pohranom podataka videonadzora. Štite se protuprepadnim i protuprovalnim sustavima za CD i nadzor alarma, neprekidnim videonadzorom s pohranom. Manipulativni novac pohranjuje se u kase ili ladice s vremenskom odgodom otvaranja. U sva vozila ugrađen je GPS sustav praćenja.

Ostale ustanove na koje se odnosi istoimeni zakon:

7. Poslovnice Hrvatske lutrije
8. Mjenjačnice i mjenjačka mjesta

8.1. Mjenjačnice kao samostalni objekti čija je osnovna djelatnost mjenjački posao

8.2. Mjenjačnice koje uz mjenjačku djelatnost obavljaju i druge poslove

9. Kladionice
10. Kreditne unije
11. Automat klubovi
12. Zlatarnice i poslovnice za otkup dragocjenosti
13. Kasina
14. Objekti pravnih osoba ili obrta s uplatno isplatnim transakcijama gotovog novca

4. SIGURNOSNE PRIJETNJE U FINANCIJSKIM USTANOVAMA

Financijske ustanove i objekti u kojima se na dnevnoj i tjednoj bazi radi s većom količinom novca i gdje je isti novac u stalnom opticaju, uvijek su bili mete manjih ili većih oblika ugrožavanja kao što su pljačke i otuđivanja. Razbojništva s prijetnjama oružjem, obijanja bankomata, velike pljačke banaka s razrađenim planovima, do sitnijih krađa osoba koje su upravo podigle novac na bankomatima itd. Principi razbojništava baziraju se na iznenadnim i brzim ulascima u objekte, u kojima se djelatnici tih istih objekata „zamrznu“ te tako ne stignu i ne znaju pravovremeno reagirati na isto. U principu su to iznenadni ulasci više osoba s oružjem uz uporabu sile ili prijetnjom uporabe sile. Obično su razbojnicima cilj takozvani „laki objekti“, budući da su im kao takvi manja prijetnja, brže otuđivanje bez velikih posljedica, gotovo nepotrebno planiranje same pljačke, mali objekt, malo zaposlenih, veća količina novaca je stalno u opticaju, npr. mjenjačnice i slični objekti. [14]

U slučaju pokušaja pljački objekta, bitno je da su službenici i zaštitari pribrani, ponašaju se profesionalno i prema uputama u slučaju pljački i procedura na radnom mjestu, te nikako ne dati povoda razbojniku za upotrebu sile i slično. Statistički gledano, razbojnici obavljaju pljačke najviše preko tjedna, radnim danima, budući da je tada novca najviše u opticaju, a vikendima se taj novac većinom transportira u regionalne podružnice ili u glavnu banku u trezor za pohranu. Pljačke su također učestalije u vrijeme blagdana, posebice Božića i Nove godine. [19] [42]

Govoreći o fizičkim razbojništvima te krađama novca i vrijednosti, nikako ne smijemo zaboraviti spomenuti i *cyber* napade te krađe velikih količina novčanih vrijednosti putem interneta i zlođudnih programa. *Cyber* kriminal je u Ujedinjenom Kraljevstvu 2015. godine porastao na 53% i tako prestigao klasični kriminal.[20] [43]

Napadač u naslonjaču i putem računala, računalnog programa i tehnologije vrši napade na online trgovanje novcem ili na programe i sustave banaka kojima vrše transakcije novcima. Napadi se događaju krađama informacija klijenata, njihovih računa, ubacivanjem u tok novca i transakcije bankovnih programa. Napadač se služi

[19] Podaci o izvršenim razbojništvima, razbojničkim krađama, teškim krađama i krađama prema statistici i analitici MUP RH – Statistički pregled 2015.
[20] The UK’s Office of National Statistics – Statistički pregled 2016.

zloćudnim programima i metodama s pomoću kojih novac s korisničkih računa preusmjerava na svoj zaštićeni račun. Može se koristiti programima i metodama napada koje je sam izradio, razradio i ubacio u tok novca (ukoliko se radi o vrhunskim stručnjacima za *online* krađe) ili je ilegalno nabavio zloćudni program i s njegovim programerom vrši otuđivanje te isti plijen dijeli s osobom od koje je nabavio program. Za velike planove i programe ubacivanja u velike financijske institucije, ipak je potreban tim stručnjaka s dobro razrađenim planom i programom, koji se može što neprimjetnije ubaciti u transakcije i rad financijske institucije. Najozloglašeniji hakeri i napadači djeluju iz Rusije, Kine, Vijetnama.[23]

5. PROJEKTIRANJE SUSTAVA ZAŠTITE

Projekt je jedinstveni pothvat koji ima jasno zacrtani cilj, krajnji rezultat, trajanje cjelokupnog projekta i najvažnije od svega, svoj proračun. Na proračun se odnose financijski aspekti, te ljudsko-tehnička podrška.

Projekt sustava zaštite predstavlja dokumentacija koja nam daje tehničko rješenje kompletnog sustava za zaštitu štićenog objekta, njegovu učinkovitost u obrani od potencijalnih prijetnji, pravovremenog upozoravanja na moguće prijetnje, te mogućnost ažuriranja. Bitno je da projektom utvrdimo sve moguće propuste sustava zaštite i otklonimo ih prije faze realizacije, kako se ne bi dogodilo da greška može imati ljudske ili materijalne posljedice.

Prema važećem pravilniku[21] provedbu tehničke zaštite podrazumijeva:

1. snimku postojećeg stanja štićenog objekta i analizu problema s ocjenom
2. izradu prosudbe ugroženosti
    a. izradbu sigurnosnog elaborata
3. definiranje projektnog zadatka
4. projektiranje sustava tehničke zaštite
5. izvedbu sustava tehničke zaštite
6. stručni nadzor nad izvedbom radova
7. obavljanje tehničkog prijama sustava tehničke zaštite
8. održavanje i servisiranje sustava tehničke zaštite
9. uporaba sustava tehničke zaštite.

Snimkom postojećeg stanja štićenog objekta i analizu problema s ocjenom donosimo zbirnim skupom podataka o:

- postojećim mjerama zaštite
- broju, tipu i načinu izvršavanja dosadašnjih štetnih događanja
- visini šteta izazvanih dosadašnjim događanjima.

[21] Pravilnik o uvjetima i načinu provedbe tehničke zaštite (Narodne novine, 198/2003.)

Prosudba ugroženosti štićenog objekta izrađuje se primjenom pravila u provedbi tehničke zaštite.

Ta priznata pravila odgovaraju hrvatskim normama, a pravila koja se ne nalaze u okvirima hrvatskih normi i pravilnika, njih nadopunjujemo međunarodno priznatim normama po standardima ISO, EN i IEC[22], te druge specijalizirane norme. [14]

Prema pravilniku[23], prosudba ugroženosti štićenog objekta izrađuje se na temelju podataka o:

1. vrsti, namjeni, veličini i izgledu objekta, lokaciji i okruženju te građevnim i ostalim svojstvima objekta
2. vrsti i broju stalnih i povremenih korisnika
3. režimu rada i načinu korištenja objekta
4. opremi, predmetima i dokumentima koji će se u objektu nalaziti ili se već nalaze te stupnju rizika od njihova oštećenja, otuđenja ili uništenja.

Pravne i fizičke osobe koje se nalaze u registru Republike Hrvatske za obavljanje poslova tehničke zaštite, na osnovu prikupljenih podataka i analize štićenog objekta, isti kategoriziraju.

Kategorizacija štićenih objekata:

1. I. kategorija - NAJVIŠI STUPANJ ZAŠTITE
2. II. kategorija - VISOKI STUPANJ ZAŠTITE
3. III. kategorija - VIŠI STUPANJ ZAŠTITE
4. IV. kategorija - SREDNJI STUPANJ ZAŠTITE
5. V. kategorija - NIŽI STUPANJ ZAŠTITE
6. VI. kategorija - MINIMUM ZAŠTITE.

[22] ISO (International Organization for standardization) – Međunarodna organizacija za standardizaciju je međunarodno tijelo za donošenje normi.
IEC (International Electrotechnical Commission) – međunarodna elektrotehnička komisija za donošenje međunarodnih normi za elektroničke tehnologije.
EN (European standard) – oznaka za normu koja je standardizirana prema ESO (European Standardization Organizations)

[23] Pravilnik o uvjetima i načinu provedbe tehničke zaštite (Narodne novine, 198/2003.)

Nakon što smo procijenili i izradili prosudbu ugroženosti, nastavljamo idući korak projektiranja sustava zaštite, a taj slijedeći korak je izrada sigurnosnog elaborata, kojim određujemo razinu tehničke zaštite, integralne zaštite i povezanost svih tehnoloških sustava.

Sigurnosnim elaboratom utvrđujemo:

1. zahtjevi koje moraju ispunjavati sustavi koji nisu sustavi tehničke zaštite, ali utječu na sigurnost objekta i pouzdan rad sustava tehničke zaštite
2. građevni i slični zahtjevi od značaja za pravilan i pouzdan rad sustava tehničke zaštite.

Slijedeći korak koji slijedi nakon sigurnosnog elaborata je projektni zadatak, čime utvrđujemo slijedeće:

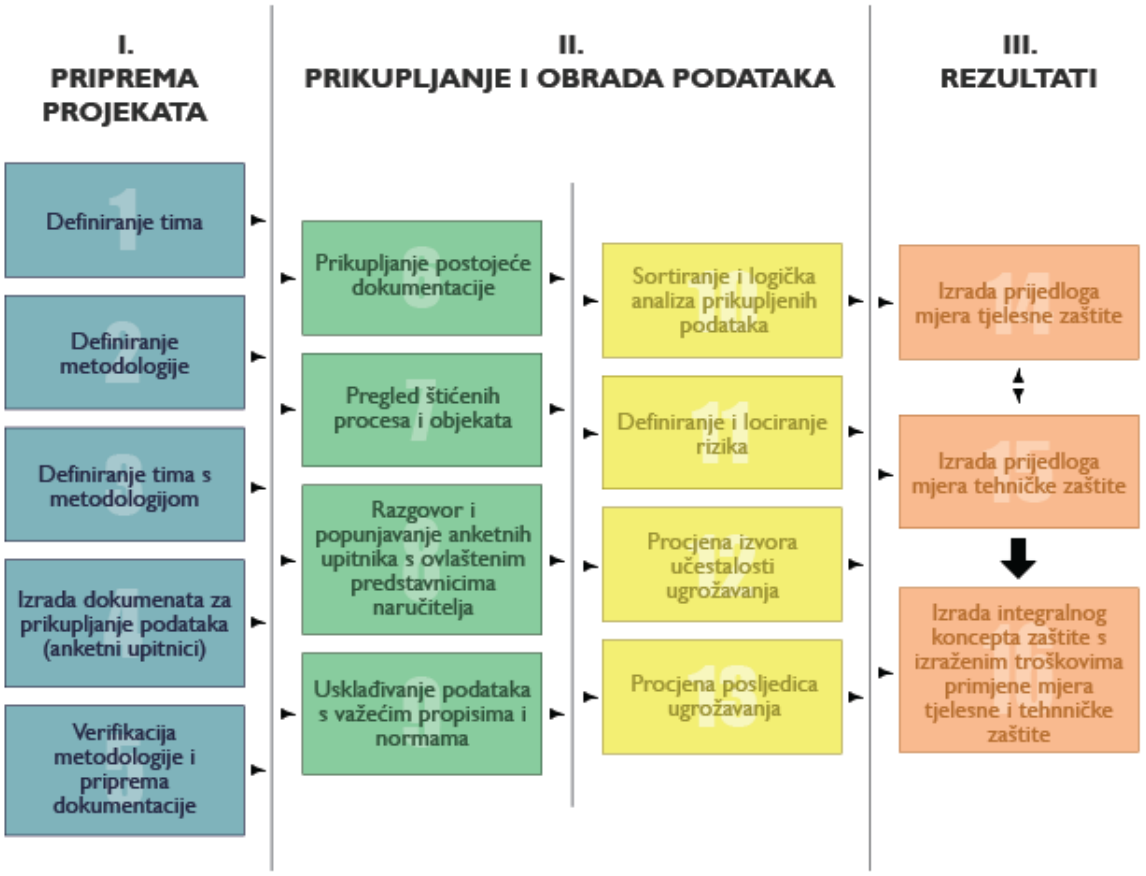
1. vrsta tehničke zaštite
2. smještaj centra tehničke zaštite
3. smještaj uređaja i opreme
4. način polaganja instalacija.

Projektni zadatak je dokument koji je izrađen slijedeći smjernice prethodno izrađene dokumentacije i na osnovu svih zahtjeva kupca usluge, odnosno naručitelja. [15]

Projektiranje prema pravilniku[24], obuhvaća:

1. odabir vrste i opsega tehničke zaštite
2. odabir uređaja i opreme
3. razradu koncepcije tehničke zaštite
4. izradbu projektne dokumentacije.

[24] Pravilnik o uvjetima i načinu provedbe tehničke zaštite (Narodne novine, 198/2003.)



Slika 1. Prikaz faza izrada prosudbe ugroženosti, sigurnosnog elaborata i projektnog zadatka [14]

Prema prilogu vidimo tri faze:

1. priprema projekta
2. prikupljanje i obradu podataka
3. rezultat.

U pripremnoj fazi definira se stručni tim koji sudjeluje u izradi dokumentacije. Rukovoditelj stručnog tima potom definira metodologiju za izvršenje zadatka, s kojom će potom upoznati kompletan tim. Nakon upoznavanja pripremaju se anketni upitnici za prikupljanje podataka.

Druga faza prikupljanja i obrade podataka obuhvaća prikupljanje projektne dokumentacije i odlazak u objekt radi detaljnog pregleda objekta i procesa koji se u

njemu i oko njega odvijaju. Ovlašteni predstavnici naručitelja svojim poznavanjem objekta i iskustvom sudjeluju u izradi procjene ugroženosti. Nakon svih prikupljenih podataka, isti podatci se analiziraju i donose se konkretni zaključci za poboljšanje mjera zaštite. Na kraju druge faze definiraju se moguća ugrožavanja i lociranje mjesta ugrožavanja, učestalost mogućih ugrožavanja i posljedice ugrožavanja.

Treća faza svodi se na izradu prijedloga mjera tjelesne i tehničke zaštite objekta te primjenu sigurnosnih standarda kako bi se moguća ugrožavanja svela na minimum.

5.1. Sadržaj projekta tehničke zaštite

Prilikom projektiranja nekog zaštitnog sustava, definiramo osnovne elemente toga projekta. Ukoliko se radi o financijskoj ustanovi koja se gradi nova od temelja, projekt sustava tehničke zaštite potrebno je implementirati od samog početka, od početnog smještaja prostorija, pa sve do završne ugradnje tehničke zaštite, ovisno o vrsti, veličini i predviđenom prometu. Treba voditi računa od instalacija, pozicioniranja, odrediti vrstu zaštite za pojedine prostorije, kao i za cjelokupni objekt. Implementiranje sustava tehničke zaštite puno je zahtjevnije za projektanta ukoliko se radi o građevinama koje nisu namijenjene prilikom gradnje da budu objekti za financije, te zbog toga daju veći izazov projektantima prilikom projektiranja sustava, kako bi ispunili sve sigurnosne zahtjeve, pogotovo ako se radi o višim kategorijama štićenog objekta.

Projektantu su bitne slijedeće informacije za izradu projekta:

1. građevinski projekt građevine.
    - Kao što se ranije navelo, ako se radi o izgradnji nove građevine, trebao bi biti uključen od faze projektiranja zgrade, kako bi lakše implementirao sustav u istu. Ukoliko se radi o gotovoj građevini, mora biti upoznat sa stvarnim stanjem građevine. Obavezno je da je upućen u cjelokupni projekt građevine, bez obzira što će se štititi samo jedno mjesto ili dio te građevine.
2. odrediti vrstu, raspored i opseg mjera sustava zaštite
3. potrebno je opisati funkcije uređaja zaštite te analizirati njihovu međusobnu komunikaciju i djelovanje
4. definiranje minimalnih tehničkih specifikacija uređaja

5. opisati rad sustava u cjelini i pojedinačno po sustavima
6. izrada grafičkog rješenja sustava
7. izrada troška investicije. [14]

Projekt dokumentacije tehničke zaštite je poslovna tajna i kao takav ne smije se iznositi.

Detaljna razrada rješenja izvedenog projekta:

1. tehnički opis sustava, opis rada, princip rada pojedinih komponenti i komunikacija s drugim sustavima
2. opis povezanosti različitih sustava tehničke zaštite
3. detaljno opisan prikaz tehničkih specifikacija kompletne opreme
4. izrada proračuna elektroinstalacija i njenih komponenti
5. opis izvedbe elektroinstalacija projektom
6. postavljanje i povezivanje opreme tehničke zaštite prateći upute proizvođača
7. grafičko prikazivanje rasporeda uređaja, s instalacijama i shemama spajanja sustava
8. nakon ispunjenih prethodnih sedam koraka, može se iskazati popis uređaja, opreme i radova s njihovim specifikacijama.

Zakonska obaveza je da se sustavi tehničke zaštite moraju održavati i u roku od minimalno jednom godišnje moraju servisirati, a te poslove smiju obavljati samo ovlaštene pravne osobe za obavljanje poslova tehničke zaštite.

Nakon izrade izvedbenog projekta, sljedeći korak je izvođenje sustava zaštite uz stručni nadzor.

Izvođenje tehničke zaštite podrazumijeva:

1. izvedbu instalacija
2. ugradnju uređaja i opreme
3. programiranje, podešavanje i ispitivanje sustava te njegovo puštanje u probni rad
4. verifikacija uređaja i opreme, sustava i tehnički prijem istih
5. izradbu uputa za rukovanje sustavom tehničke zaštite
6. obuku osoblja.

Pripremne radnje za instalacije mogu obavljati pravne osobe koje ne moraju imati ovlasti za obavljanje tehničke zaštite.

Instalacije tehničke zaštite moraju biti izvedene prema projektu koji je u skladu s Pravilnikom o uvjetima i načinu provedbe tehničke zaštite.

Nakon ugradnje i ispitivanja instalacija tehničke zaštite, ugrađuju se uređaji i oprema koji se podešavaju prema uputama i dokumentaciji proizvođača.

Probnim radom se ispituje stabilnost i rad sustava koji, ukoliko ispunjava sve uvjete, dobiva certifikat. Osobe koje će rukovati i upravljati sustavom, moraju biti obučene za rad s istim, čiju obuku odrađuje pravna osoba koja je ugradila sustav. [14]

6. SUSTAVI TEHNIČKE ZAŠTITE OBJEKTA

Tehnički sustavi dijele se na aktivnu i pasivnu zaštitu, gdje je aktivna elektronička, a pasivna mehanička. Koji će se od ovih sustava koristiti najviše ovisi o procjeni ugroženosti objekta. [13]

Protuprovalni sustavi se koriste za sprječavanje neovlaštenog pristupa, a neki od primjera protuprovalnih sustava mogu biti protuprovalna vrata, mehanizmi protiv obijanja, sefovi, trezori, itd. Protuprepadni sustavi služe za sprječavanje pokušaja razbojništva, u kojem alarmni sustav jakim zvučnim signalom alarmira okolinu i razbojnika te ih tako sprječava, a uz to privlači moguće svjedoke i očevidce. Uz to centralni dojavni sustav CDS dojavljuje zaštitarskoj službi ili nadležnoj policijskoj postaji da se dogodio neovlašteni pokušaj ulaska u štićeni objekt te se upućuje interventnu ekipu na mjesto događaja.

Također postoje razni sustavi zaštite od neovlaštenog iznošenja novca, vrijednosti, predmeta ili robe izvan objekta, koji registrira krađu, uzbunjuje pomoću alarma zvučnim signalom zaštitara koji se nalazi u štićenom objektu. To su sustavi elektroničke zaštite od neovlaštenog iznošenja EAS[25], koji osim te funkcije ima i funkciju kontrole količine robe, lakše praćenje robe s istekom roka trajanja, stanja robe itd. [16]

Sustavi centralne dojave (CDS) i sustavi alarmne signalizacije su složeniji oblici tehničke zaštite koje se rade po projektu i izvode identično prema istom, a način postavljanja i njegovu funkciju određuje procjena ugroženosti objekta.

Najčešći sustavi zaštite koje možemo primijetiti u objektima su sustavi videonadzora CCTV. Njegove zadaće su praćenje zaštitarske službe unutar objekta, svojom pojavom odvraća potencijalne razbojnike od provale, a u slučaju provale i razbojništva služi kao video materijal za očevid, te kao sustav snimanja i video pohrane.

U ustanovama i institucijama najviše razine zaštite nalaze se detektori metala i rendgenski uređaji za kontrolu neovlaštenog unošenja potencijalnih predmeta za izvršenje krađe (oružja, predmeta za obijanje, eksplozivnih naprava itd.).

[25] EAS (electronic article surveillance) – uređaji koji pobuđuju alarmni sustav prilikom neovlaštenog iznošenja predmeta izvan objekta

Vrste zaštite možemo podijeliti prema:

1. Vanjska zaštita – ova zaštita se odnosi na zaštitu koja se nalazi oko štićenog objekta, a omogućuje ranu detekciju ulaska u objekt. Ona mora omogućiti nesmetano kretanje, a prilikom projektiranja i izrade mora se voditi obzira o vanjskim utjecajima na istu. To su ograde, zidovi i razne prepreke na koje se postavljaju infracrvene barijere[26], mikrovalne barijere[27], elektromagnetski detektori[28], video detektori kretanja[29].
2. Periferna zaštita – sustav zaštite na samoj građevini koji detektira svaki nasilni pokušaj ulaska u istu, pokušava spriječiti provalnika na sami čin nasilne provale. Periferni sustav zaštite mora biti isključen dok se u štićenom objektu odvijaju kretnje unutar radnog vremena. Ovi sustavi su elektromagnetski i magnetski kontakti, infracrveni senzori te detektori loma stakla[30] i slično.
3. Prostorna zaštita – odnosi se na unutarnju zaštitu objekta, čiji je cilj detekcija neovlaštenog kretanja unutar objekta. Ovaj sustav zaštite detektira razbojnika i neovlaštene kretnje unutar samog objekta ukoliko je razbojnik zaobišao prva dva elementa zaštite, a odnosi se na prostorije u kojima nije dozvoljeno kretanje izvan radnog vremena. Ove sustave zaštite čine PIR (pasivni infracrveni) detektori[31], infracrveni i ultrazvučni detektori[32], detektori zvuka[33] i slično.

[26] Aktivna infracrvena barijera – sustav zaštite od prijemnika i predajnika, u kojem provalnik prekine emitirani infracrveni snop zraka i tako aktivira alarm.
[27] Mikrovalne barijere – sustavi koji se sastoje od prijemnika i predajnika, najčešće su to ukrasni stupovi koji emitiraju mikrovalni snop valova, koji prilikom prekidanja vala aktivira alarm.
[28] Elektromagnetski detektor – ovaj sustav detektira promjene elektromagnetskog polja unutar područja svoje primjene. Elektromagnetsko zračenje ovih sustava nemaju štetan utjecaj na čovjeka.
[29] Video detektori kretanja – sustav video nadzora koji u svom vidnom polju otkriva kretanje , te zvučnim ili svjetlosnim signalom dojavljuje da su se dogodile kretnje u perimetru zaštite.
[30] Detektor loma stakla - uređaj koji prepoznaje specifične frekvencije koje prouzrokuje pucanje stakla.
[31] PIR detektor – je vrsta infracrvenog senzora koji emitira infracrvenu zraku u svome vidnom polju.
[32] Ultrazvučni detektori – emitiraju ultrazvučne valove koji se odbijaju po prostoru, ako u prostoru nema kretnji, valovi se odbijaju neometano, međutim ako se netko kreće po prostoru, on izobliče valove i tako aktivira alarm.
[33] Detektori zvuka – funkcioniraju na principu detektora loma stakla, samo na drugim frekvencijama.

4. Protuprepadna zaštita – njezin cilj je da aktivira signalizaciju (tihu ili zvučnu) u slučaju pokušaja razbojništva u financijskom objektu ili drugog ugrožavanja štićenog objekta. Ova vrsta zaštite se mora fizički aktivirati, na primjer u slučaju razbojništva na banku, službenik koji je napadnut ili službenik koji je uočio pokušaj razbojništva, pritiskom na tipkalo aktivira tihi alarm. Protuprepadni sustavi u objektima visokog rizika, moraju automatski aktivirati snimanje razbojništva koji služi kao dokaz poslije razbojništva. Ove sustave čine ručne panik šine, senzori novčanog snopa (kada se makne snop sa senzora koji se nalazi na određenoj novčanici, on aktivira protuprepadnu zaštitu), video kamere, uređaji koji ispuštaju dimnu zavjesu unutar prostora koja onemogućuju kretanje, detektori za iznošenje novca van objekta, koja prilikom bijega s mjesta počinjenja, bojom označuju razbojnika i ukradeni novac koji su otuđili.
5. Kontrola pristupa – njezin je zadatak onemogućavanje neovlaštenog ulaska u štićeni objekt. Zaposlenici, službenici i zaštitari posjeduju fizičke identifikacijske kartice, koje im omogućuju da evidentiraju svoj ulazak i kreću se unutar ograničenih područja. Identifikacija može biti biometrija, razni bar kodovi, QR kodovi, identifikacijske kartice i slično. Najčešće se koriste RFID (radio-frekvencijski identifikator) čitači za identifikaciju putem kartica.
6. Zaštita štićenih predmeta – njihova funkcija je da registriraju i signaliziraju pokušaj razbojništva predmeta koji se nalazi u štićenom objektu. Štićeni predmet se nalazi u prostoriji u kojoj je omogućeno slobodno kretanje, međutim ako ova vrsta sustava detektira pokušaj otuđenja tog predmeta, aktivira se alarm. [13]

6.1. Protuprovalni sustavi

Glavni zadatak protuprovalnih sustava je da detektira i registrira svaki pokušaj neovlaštenog ulaska u objekt. Glavna karakteristika i prednost protuprovalnih sustava je jednostavnost njihove izvedbe i instalacije, te njegova povoljna cijena. Inače su kao sustavi najrasprostranjeniji, najbrže se razvijaju, izrazito su povoljni za kućanstva, te kao takvi su najbolje rješenje za zaštitu imovine. Danas se po vrlo niskim cijenama može kupiti i instalirati protuprovalni sustav. Najčešće su to video nadzori, kamere za

bežično povezivanje s mobilnim ili računalnim aplikacijama, te ih se kao takve može lako povezati i u svako doba dana pregledati.

Elementi protuprovalne zaštite:

1. uređaji za detekciju
2. centralni sustav koji prima i obrađuje signal
3. uređaji za uzbunjivanje i prenošenje informacija.

Uređaje za detekciju dijelimo na detektore za:

1. perimetarsku detekciju
2. prostornu detekciju
3. detekciju specifičnog objekta. [13]

6.1.1. Uređaji za perimetarsku detekciju

Ove uređaje za zaštitu možemo opisati kao uređaje koji predstavljaju prvu liniju obrane od napada na objekt. To može biti ograda, vrata, prozori, zidovi itd. Uređaje za perimetarsku zaštitu možemo podijeliti na:

1. Magnetski kontakti – sastoje se od preklopnika i magneta, postavljaju se na objekt tako da su u blizini jedan drugoga, budući da djeluju u magnetskom polju kako bi djelotvorno obavljali svoju funkciju. U slučaju razdvajanja, preklopnik izlazi iz magnetskog polja djelovanja i tako se aktivira alarm. Najčešće se postavljaju na vrata, prozore, te druge objekte i uređaje koje je potrebno zaštititi od neovlašten ulazak u područje.
2. Pasivni infracrveni detektori – rade na principu prijema infracrvenog zračenja. Infracrveno zračenje detektora je povezano s okolinskom temperaturom objekta, dok je čovjek pomični izvor infracrvenog zračenja koje utječe na okolinu infracrvenog polja zračenja. Ukoliko razbojnik pokuša izvršiti razbojništvo u objektu u kojem je instaliran pasivni infracrveni detektor, ulaskom u područje infracrvene zrake prekida istu i uključuje alarm. Ovisno o vrsti, mogu imati jednu ili više zona ili segmenata detekcije. Pogodni su za prostore od 10 do 120 m^2.

3. Detektori loma stakla – rade na principu da prilikom loma stakla, događaju se mehaničke oscilacije koje registrira piezoelektrični senzor unutar detektora i aktivira alarm. Prilikom loma stakla aktivira se određena frekvencija koju detektor primi i ako ta frekvencija izađe izvan zadane, ona aktivira alarm. Jednostavni detektori loma stakla primaju samo određeni frekvencijski raspon, dok oni kompliciraniji imaju ugrađeni digitalni procesor signala koji obrađuje veću količinu podataka u kraćem vremenu.
4. Alarmna stakla – specifična stakla koja imaju kroz svoju dužinu unutar samih ugrađenu tanku nit. Prilikom loma stakla, ta nit se prekida i aktivira alarmni sustav. Koriste se najčešće na objektima s velikim izlozima i staklenim površinama.
5. Seizmički detektori – rade na istom principu kao i detektori loma stakla, međutim njihovo je djelovanje na detekciji provale s čvrstim predmetima za provalu (bušilice, brusilice, eksplozivni materijali i slično), koji prenose vibracije na predmet ili objekt, te tako uzbuđuju alarm. Njihovo djelovanje i način detekcije pogodan je za trezore, sefove itd.
6. Detektori za zaštitu umjetnina – djeluje na principu gravitacijske sile. Umjetnina se postavi na postolje ili držač koji u sebi sadrži nit koja je povezana sa senzorom koji reagira na promjenu mase, frekvenciju i pritisak. Kada se promjeni zadana sila predmeta, senzor očitava pomake i reagira uzbuđivanjem alarma. [13]

6.1.2. Centralni uređaji

Alarmna centrala ili centralni uređaj je srce protuprovalnog sustava. Na nju se spajaju svi detektori objekta, gdje se ulazni podatci obrađuju i reagiraju te aktiviraju određene mjere u slučaju neovlaštene kretnje. Uz detektore, na centralni uređaj se povezuje upravljački uređaj za upravljanje sustavom, te programiranje i podešavanje istog. Na upravljačkom uređaju korisnik se prijavljuje, uključuje, isključuje i upravlja sustavom, kao cjelinom, a može i pojedinačnim segmentom sustava. Svaki korisnik ima svoj profil, zaporku, koja ga identificira i daje mu mogućnosti koje su mu programom zadane. Neki korisnici imaju ograničen pristup koji im dopušta samo djelomično upravljanje. Pojedini korisnici imaju potpunu kontrolu i mogućnost višestrukog

upravljanja, unošenja promjena, programiranja, dok neki od njih samo mogu uključivati i isključivati sustav. Najveću ovlast u sustavu imaju instalateri koji su sustav podesili, postavili i koji ga održavaju. Također se cijeli sustav može programirati tako da instalateri nakon puštanja u rad više taj sustav ne mogu isključiti jednom kada je sustav pokrenut i pušten u rad. Svaki unos zaporke korisnika bilježi se u centrali. Sustav je povezan na CDS (centralni dojavni sustav) u ovlaštenoj tvrtki, koji prati rad cjelokupnog sustava, od uključivanja, isključivanja, periodičnih servisa, ispitivanja itd. CDS u ovlaštenoj tvrtki prikuplja sve podatke koji mu dođu od alarmnih centrala te na osnovu istih može izraditi statističke podatke na tjednoj, mjesečnoj ili godišnjoj bazi. Alarmna centrala i digitalni komunikator međusobno komuniciraju u dva smjera, međusobno šalju informacije, imaju mogućnost daljinskog upravljanja, programiranja te ažuriranja iz centralnog dojavnog sustava. Kod suvremenih alarmnih centrala ulazak je moguć samo određenim putem, to jest aktiviranje detektora određenim redoslijedom, u suprotnom se aktivira alarm. Alarmne centrale imaju svoje samostalno napajanje u slučaju isključenja iz mrežnog rada, koje automatski preuzima rad u slučaju nestanka struje i može održavati rad sustava i do 24 sata. Alarmna centrala ima funkciju zaštite detektora u slučaju pokušaja sabotaže, budući da svi detektori moraju biti spojeni na centralu, bilo u slučaju da je alarmni sustav isključen ili uključen, detektori moraju imati detekciju u slučaju pokušaja isključenja, prekida s napojnim ili signalnim kablovima, te u slučaju otvaranja detektora. [14]

6.1.3. Uređaji za uzbunjivanje i prenošenje informacija

Nakon primitka signala, njegove obrade u centralnom uređaju, dolazimo do trećeg dijela sustava koji odlučuje hoće li se alarm aktivirati po primljenom signalu.

Uređaje za uzbunjivanje i prenošenje informacija čine:

1. unutarnja sirena
2. vanjska sirena s bljeskalicom
3. digitalni dojavljivači
4. izlazni prekidači za aktivaciju drugih sustava tehničke zaštitu.

1. Unutarnja sirena – smještena je unutar objekta na mjesto gdje je što teže vidljiva i dohvatljiva. Iako treba biti sakrivena što je više moguće, opet mora imati dovoljno prostora kako bi se zvučni valovi mogli ravnomjerno raspršiti po štićenom objektu i prostoru. Njezina primarna funkcija je ta da kada je aktivirana stvara jaki zvučni signal koji skreće pozornost okoline na objekt i stvara psihološki pritisak na provalnika da je uhvaćen u akciji.

2. Vanjska sirena s bljeskalicom – postavlja se na vidljivo mjesto na štićenom objektu, a također da je što teže dohvatljiva. Ovaj element ima dvostruko kućište, koje onemogućuje lak pristup sireni. Unutar kućišta sirene nalazi se napajanje koje preuzima rad u slučaju isključenja s mreže, a pri pokušaju sabotiranja sirene, aktivira se rad vlastitog napajanja i aktivira zvučnu uzbunu. Osim zvučne uzbune sirene, postoji i bljeskalica daje vizualni signal razbojništva na objekt.

3. Digitalni dojavljivač – njegova svrha je da u što kraćem vremenskom roku alarmni signal u centralni dojavni sustav. Moderni digitalni dojavljivač u jako kratkom vremenu može prenijeti više stotina informacija. Osim svoje primarne funkcije, digitalni dojavljivač dojavljuje:

- aktivaciju i deaktivaciju alarmnog sustava s datumom i vremenskim unosom, te korisnika koji je obavio isto
- nestanak i povratak mrežnog rada, uključenje rezervnog napajanja
- pokušaj daljinske deaktivacije alarma
- periodične testove
- tehničke greške u sustavu
- pokušaj sabotaže sustava ili jednog od njegovih elemenata.

4. Izlazni prekidači – programirani su i povezani na alarmnu centralu, a u slučaju aktiviranja alarma aktiviraju i uređaje koji u trenutku alarma odvraćaju provalnika. Povezuju se s vanjskom i unutarnjom rasvjetom, ozvučenjem, klimatizacijskim sistemima itd. Na primjer, videonadzor koji neprekidno snima objekt, a spojen je na izlazni prekidač. Kada se pobudi alarm, izlazni prekidač prebacuje sustav video nadzora iz normalnog rada u alarmni način, koji snima uživo snimku u više slika u sekundi, te tako može bolje dati informacije za očevid.

5. Sustavi za aktivaciju dima kao element protuprovale – princip sustava je taj da u slučaju provale, aktivira se dim u štićenom prostoru. Oni su povezani s alarmnim sustavom, koji ako se aktivira, puni štićeni prostor gustim neškodljivim dimom, te tako zadržava provalnika u prostoru dok ne dođe interventna služba. Cilj je da se spriječi provalnika za nastavak krađe te da mu se otežа i onemogući izlazak iz prostora dok ne dođe policija. [15]

6.1.4. Analiza sustava zaštite bankomata

Prema MUP-ovim statistikama 2013. godine, počinjena je 21 provala bankomata, a 2014. i 2015. godine 14. Najčešće su to bankomati koji se nalaze izvan financijskih institucija.

Podatci iz MUP-a nam govore da su upravo ti eksterni bankomati meta zbog toga što se u čestom broju slučajeva nalaze na javnim površinama, radi bolje dostupnosti korisnicima. Nije rijetkost da bankomate susrećemo na perifernim dijelovima grada, slabo osvjetljenim mjestima, mjestima s malom fluktuacijom prometa, pa su kao takvi meta razbojnicima. Neki od primjera fizičkih napada na bankomate su bušenja bankomata, upotreba raznih alata za obijanje, izvlačenje cijelog bankomata pomoću automobila i užeta, te korištenje plina za otvaranje bankomata. [18]

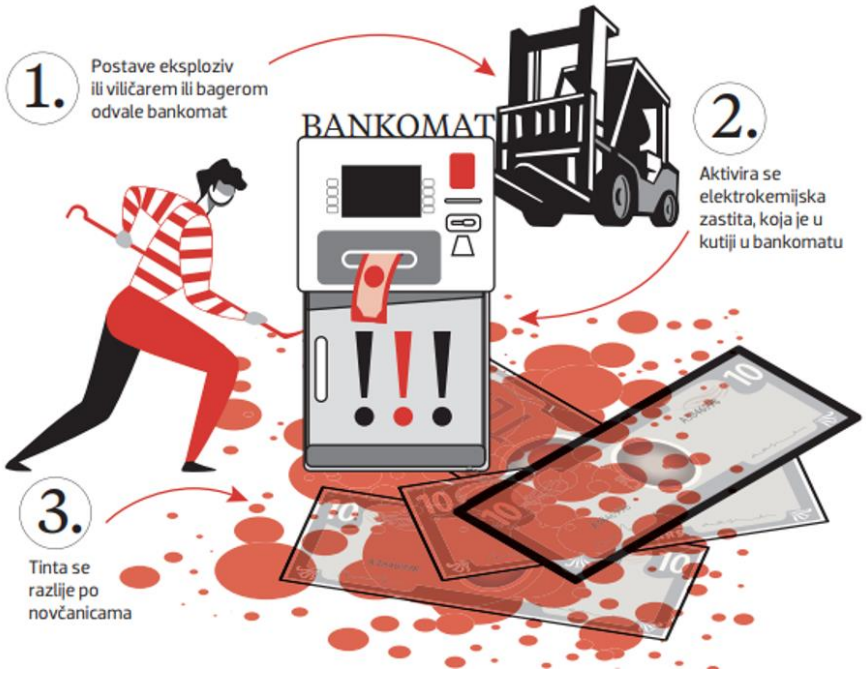
Sustav inteligentne neutralizacije novca (IBNS[34]) je jedna od mjera zaštite, odnosno uništavanja „plijena“. Rade na principu da kad sustav detektira pokušaj obijanja, aktivira spremnik s bojom, koji se nalazi u prostoru za pohranu novčanica. Tinta se razlije po novčanicama i tako ih oboja i uništi. Tinti se dodaje forenzički marker, da u slučaju ispiranja boje s novca, marker ostaje na novčanicama, koji služi forenzičarima u istrazi.

Jedna od tehnika uništavanja novčanica koja se razmatra je sustav neutralizacije ljepilom. Funkcionira isto na principu kao i sustav s tintom, samo je drugo sredstvo koje se nalazi u spremniku. Međutim ljepilo može predstavljati opasnost od požara, budući

[34] IBNS - Intelligent banknote neutralisation system (inteligentni sustav neutralizacije novčanica)

da raspršivanje čestica ljepila u zraku stvara potencijalno zapaljivu smjesu. Ovi sustavi su još u fazi izrade.

Analizom procjene ugroženosti možemo utvrditi u kakvom se okruženju nalazi. Ako se bankomat nalazi na lokaciji visokog rizika, prvi korak je premještaj bankomata na lokaciju sigurnog okruženja. Ukoliko bankomat nije moguće premjestiti, treba poduzeti mjere povećanja sigurnosti. Neke od mjera sigurnosti su postavljanje protuprovalnog zaslona, bolja ulična rasvjeta, rasvjeta područja oko bankomata, pojačanje nadzora bankomata i područja oko bankomata, postavljanje sustava za zamagljivanje prostora oko bankomata itd. [19]



Slika 2. Sustav elektrokemijske zaštite [32]

6.2. Protuprepadni sustavi

Protuprepadni sustavi zaštite imaju svrhu tihog dojavljivanja opasnosti u štićenim objektima pomoću fizičkih dojavljivača (tipkala). Ovaj sustav kombinira tjelesnu, tehničku i mehaničku zaštitu.

Uređaji i detektori protuprepadne zaštite većinom se spajaju na alarmnu centralu, na koju su spojeni protuprovalni detektori, te u tom slučaju sve informacije o pokušaju

provale ili prepada se prikupljaju na jedno centralno mjesto. Osim tihog načina dojave, protuprepadni sustavi također se koriste i za aktiviranje ostalih sustava tehničke zaštite. Tako je moguće da npr. u trenutku pokušaja provale protuprepadni sustav aktivira kameru da iz pasivnog stanja prijeđe u aktivno i započne sa snimanjem. [15]

6.2.1. Elementi sustava protuprepadne zaštite

Oni su sljedeći:

1. ručna tipkala
2. bežična tipkala
3. alarmne šine (nožne)
4. detektori zadnje novčanice
5. kase i sefovi s vremenskim kašnjenjem
6. nagazni tepih
7. blindirana dvostruka vrata s detektorom metala
8. sustavi za bežično aktiviranje dimne zavjese.

Slika 3. Ručno tipkalo, bežično tipkalo, alarmna nožna šina, sef s vremenskim kašnjenjem, nagazni tepih, sustav za bežično aktiviranje dimne zavjese [33, 34, 35, 36, 37, 38]

Ručna tipkala se često koriste u sustavima protuprepada. Jednostavni su za implementaciju i prenose dva stanja u alarmnu centralu, prvo stanje je pasivno, a drugo aktivno u kojem je tipkalo pritisnuto i aktiviralo tihi alarm. Postavljaju se tako da su u neposrednoj blizini ugroženog osoblja, npr. ispod pulta, stola, na zid, tako da su nadohvat ruke. Zidna tipkala su koncipirana tako da ih mogu aktivirati osobe koje nisu direktno ugrožene, već su to one osobe koje su očevidci koji mogu neprimjetno aktivirati ručno tipkalo. Aktivirana ručna protuprepadna tipkala se mogu deaktivirati samo pomoću ključa.

Bežična tipkala su iste funkcije i karakteristika kao ručna tipkala, ali budući da su prenosiva, ne moraju biti vezana za mjesta koja su ugrožena. Ona se nalaze kod

potencijalno ugroženih osoba unutar štićenog objekta. Svako bežično tipkalo ima svoj identifikacijski broj koji u slučaju aktivacije omogućuje brzu lokaciju mjesta s kojeg je aktiviran alarm.

Nožne alarmne šine se postavljaju ispod šalterskog mjesta. Glavna prednost ovog elementa je ta što omogućuje neprimjetniju aktivaciju u kojoj je dovoljan lagani pritisak nogom na šinu, bez očitih primjetnih pomicanja osobe, npr. u slučaju kada razbojnik zatraži šalterskog službenika da digne ruke u zrak, on je još uvijek u mogućnosti da s nogom pritisne šinu i aktivira alarm. Isto kao i kod ručnih tipkala, moraju se ključem deaktivirati. [15]

Detektor zadnje novčanice su neprimjetni uređaji za dojavu u trenutku prepada, a dijelimo ih na mehaničke i elektroničke. Mehanički imaju ugrađen mikro prekidač u koji se umeće zadnja novčanica snopa, a postavlja se u ladicu ili na mjesto tako da je skriven od pogleda. U slučaju pljačke, napadač traži od šalterskog službenika da mu preda sav novac, te u trenutku kada radnik izvlači posljednju novčanicu, aktivira se mikro prekidač i aktivira alarm. Elektronički detektor funkcionira tako da reflektira zraku od novčanice i kada se novčanica makne s detektora i izvora svjetlosti, ona automatski aktivira alarm. Elektronički su u principu bolja opcija od mehaničkih jer su jednostavniji i mogu se postaviti da su potpuno neprimjetni.

Kase i sefovi s vremenskim kašnjenjem rade na principu kase s dvije ladice. Gornja ladica sadrži određeni dio sume novaca koji se koristi za manje isplate, a kada se ta ladica ispuni s određenom većom količinom novca, otvara se dio između gornje i donje ladice i novac se prebacuje iz gornje ladice u donju. Donji sef kase je veći i bolje zaštićen od gornjeg sefa kase. Ugrađeni sustav vremenskog kašnjenja programira se od jedne minute ili duže ako se utipka programirani kod, pa na taj način vremenski sprječava razbojnika da dođe do novca. Novčarske institucije su obavezne istaknuti obavijesti o zaštiti poslovnice sustavima tehničke zaštite.

Nagazni tepih je detektor koji može služiti kao protuprovalni, ali i protuprepadni element detekcije. Radi na principu primijenjene sile na površinu koja aktivira alarm, a postavlja se ispred ulaza u posebno štićeni prostor s upravljačkom tipkovnicom koja

uz pomoć identifikacijskog koda može u kratkom roku isključiti zaštitu te zone. Pritiskom određene sile na tepih, aktivira se predalarmno stanje koje će se uključiti u određenom vremenskom periodu ako se ne unese identifikacijski kod, a vremenski period od aktivacije nagaznog tepiha i alarmnog stanja daje signal zaštitarskom osoblju unutar objekta da je alarm uključen.

Blindirana dvostruka vrata s detektorom metala (tzv. *interlocking* vrata/kabina) su skupa ali učinkovita zaštita protuprepada, a funkcionira tako da samo jedna vrata mogu biti otvorena u isto vrijeme. Prva vrata se otvaraju, osoba ulazi u međuprostor, prva vrata se zatvaraju, detektor metala odradi provjeru i ako se ne aktivira detektor, druga vrata se otvaraju i osoba može ući u prostorije. Ovaj način zaštite je vrlo učinkovit kako kao protuprovalni element zaštite, tako je i element protuprepada, koji sprječava napadača da jednostavno uđe u prostorije banke ili nekog drugog štićenog objekta ili prostorije. Ovi sustavi su uvedeni u sve banke, a najbolji primjer *interlocking* kabina možemo vidjeti uglavnom u manjim poslovnicama.[14]

Slika 4. Interlocking sustava protuprepadne zaštite [39]

Sustav za bežično aktiviranje dimne zavjese se sastoji od mini bežičnog prijemnika koji aktivira spremnik s dimnom zavjesom. Bežični prijemnik i spremnik s dimom nalaze se

u snopu novca kako ih napadači ne mogu lako uočiti. Blizu izlaznih vrata se postavlja mini predajni uređaj koji je u dometu prijemnog uređaja. Nakon što napadač otuđi snop novca u kojem se nalazi prijemnik i udaljava se od financijskog objekta, tako povećava udaljenost između prijemnog i predajnog uređaja i kada ta dva uređaja izađu iz dometa, aktivira se spremnik s dimom koji oboji snop novca i označi napadača koji je otuđio novac. [14]

7. SUSTAV ZA KONTROLU PRISTUPA

Sustav za kontrolu pristupa je jedan od najvažnijih elemenata za zaštitu financijskih institucija, kao i ostalih objekata s visokim rizikom od razbojništva i drugih nasilnih kaznenih djela. Oni kontroliraju svaki ulaz i izlaz u štićene objekte ili u pojedine posebno štićene prostorije unutar objekta. Posebno važni prostori moraju imati izvedene ove sustave kontrole kako bi samo ovlaštene osobe mogle imati pristup i spriječiti svaki neovlašteni ulaz i kretnju unutar istog. Osim ograničenog pristupa neovlaštenog osoblja, svrha ovih sustava je i kontrola i evidencija svih prolazaka kroz isti, pohrana podataka o njima, alarmna stanja i operaterske aktivnosti. Ovi sustavi reduciraju troškove tjelesne zaštite i podižu stupanj zaštite na višu razinu.

Baza pohrane podataka vodi evidenciju o:

- podatci o ovlaštenoj osobi
- ovlasti kretanja u štićenom objektu
- vremenski period za kretanje u štićenom objektu
- evidencija ulaska/izlaska.

Za postavljanje sustava kontrole pristupa popunjava se slijedeći upitnik:

1. definiranje vrste i veličine ulaznog elementa registracije
2. broj i pozicija nadziranih prolaza
3. određivanje broja korisnika sustava
4. učestalost prolazaka
5. postupak izdavanja novih kartica.

Sustav kontrole pristupa mora imati protusabotažnu detekciju i neovisno napajanje. Ovi sustavi imaju veliku primjenu u raznim vrstama kontrole pristupa:

- kontrola ulaska u štićeni objekt
- kontrola ulaska na parking
- kontrola pristupa u objekte od visoke važnosti
- kontrola radnog vremena
- nadzor čuvarske službe
- kontrola kretanja liftom

- povezanost i djelovanje s ostalim sustavima tehničke zaštite.

Elementi sustava za kontrolu pristupa:

1. Ulazni elementi sustava kontrole pristupa – čine ih kodirana brava, elektronički i mehanički čitač, biometrijski čitači, te ostali elementi. Princip rada ulaznih elemenata je da omoguće pristup osobama koje su uspješno prošle registraciju ulaska, a u suprotnom onemogućile pristup neovlaštenog osoblja i svaki neovlašteni pokušaj pristupa. Ovi sustavi za omogućavanje ulaska u štićeni objekt koriste biometrijske podatke (skenere otiska prsta, zjenice oka, otisak cijelog dlana, itd.), beskontaktne naprave (pametni uređaji s beskontaktnim mogućnostima, kartice, beskontaktni ključevi, itd.). Biometrijske čitače najčešće možemo susresti u objektima visoke važnosti, financijskim institucijama, trezorima, sefovima, laboratorijima, objektima za razvoj visoke i strateške tehnologije itd.
2. Centralni uređaj sustava za kontrolu pristupa je u principu isti kao i kod ostalih sustava tehničke zaštite, smješta se u najzaštićeniji dio objekta. Rezervno napajanje mora biti projektirano tako da s čitačima i izlaznim elementima radi potpuno sinkronizirano, da u slučaju mrežnog i rezervnog napajana omogući nesmetani izlazak zaposlenika i gostiju u što kraćem roku. Svi podatci o ovlaštenim i neovlaštenim pokušajima registracije se pohranjuju na memoriju računala i na memoriju centralnog uređaja koji je neovisan o računalu.
3. Izlazni elementi za kontrolu pristupa mogu biti :
    - električne brave
    - rasvjeta
    - protuprovalni sustav
    - video nadzor
    - dojavni uređaji.

    Princip rada je taj da nakon registriranja ulaznog elementa, omogućuje se otvaranje prolaza u štićeni prostor, deaktivira se alarmna zaštita i kretanje unutar istog prostora je omogućeno.

Često se spajaju na video nadzor na slijedeće načine:

1. Prilikom ulaska i izlaska aktivira se videonadzor koji snima uživo
2. Prilikom ulaska u prostor aktivira se određena kamera koja pokriva kretnje osobe koja se nalazi u tom prostoru. [14]

8. SUSTAV VIDEO NADZORA

Sustav video nadzora je zatvoreni sustav u kojem se prikuplja video signal s postavljenih lokacija u štićenom objektu, a samo ovlašteni ljudi imaju pristup sustavu video nadzora.

Prvi komercijalni sustav video nadzora pojavio se u SAD-u 1949. godine. Naime, prvi veliki skok u CCTV sustavu video nadzora dogodio se 1956. godine kada su u te sustave implementirane video kasete, za pohranu video zapisa. Godine 1970., prvi CCTV sustavi nadzora postavljaju se u financijske objekte, kao dodatna mjera zaštite. Drugi bitan pomak dogodio se 1990. kada se pojavljuje multipleksiranje. Ta tehnologija omogućuje istovremeno praćenje više video signala na jednom monitoru. Sve do 2006. godine koristila se analogna video tehnologija video nadzora, koju preuzimaju IP kamere visoke rezolucije, čiji sustavi spremaju video zapise u digitalnom obliku na hard diskove. Kamere visoke rezolucije omogućuju precizne video snimke s mogućnošću prepoznavanja lica. [20]

Sustavi video nadzora prema konfiguraciji dijele se na:

- Analogne sustave za video nadzor – čine ih jedna ili više kamera i monitor za nadzor tih kamera
- Analogne sustave za nadzor i snimanje – čine ih jedna ili više kamera, monitor i video rekorder za snimanje video sadržaja
- Digitalne sustave za video nadzor i snimanje – čine ih jedna ili više kamera, monitor i digitalni snimač za pohranu video sadržaja
- Mrežni nadzorni sustav – srce su ovog računala koja putem mreže prenose sliku i mogu se upravljati putem telefona.

Video nadzor ima široku primjenu, a omogućuje nam zaštitu od:

- neovlaštenog pristupa
- pristup ovlaštenih osoba unutar štićenog objekta
- nadzor u financijskim institucijama
- nadzor kriminalnih aktivnosti
- sigurnost osoba, materijalne i nematerijalne imovine

- nadzor zaposlenika i stranaka u štićenom objektu
- nadzor javnih površina i kretanje po istima
- nadzor parkirališta
- nadzor trgovina
- nadzor postrojenja
- nadzor privatnih posjeda.

Prednosti sustava videonadzora:

- ušteda na troškovima
- brzi pristup vizualnim informacijama u slučaju razbojništva
- veća pouzdanost i sigurnost u sustavu zaštite
- jednostavan nadzor i upravljanje
- jednostavnija identifikacija službenika, gostiju, zaštitara i mogućih počinitelja.

8.1. Elementi video nadzornog sustava

Suvremeni sustav video nadzora čine slijedeći elementi:

1. video kamere
2. monitori
3. uređaji za obradu signala
4. mediji za prijenos podataka
5. uređaji za analogno i digitalno snimanje i uređaji za pretvorbu digitalnog signala u analogni i obrnuto
6. pomoćni uređaji.

Video kamere su početni su i osnovni element sustava video nadzora, a možemo ga nazvati „oko“. Kamere mogu biti digitalne ili analogne. Zbog današnje digitalizacije najrasprostranjeniji je upravo digitalni način. IP ili digitalne kamere prenose video signal preko mreže sustava. Prednost im je što imaju bolju rezoluciju slike, veću povezanost kamera u kompletnom sustavu, uštedu na prostoru zbog kompaktnosti i nezahtjevnosti za povezivanje žicom, nadzor štićenog objekta s bilo kojeg mjesta i u stvarnom vremenu, pohranu podataka na tvrde diskove. Neki od nedostataka su im

nešto veća cijena, zahtjevan internet s mogućnošću protoka veće količine podataka, te mogućnost hakiranja unutar mreže.

Video monitori su uređaji koji prikazuju video signal koji putuje iz kamere preko prijenosnog medija. Imaju dosta mogućnosti podešavanja, koje im omogućuju da se svaka promjena parametra prikazuje na monitoru. Na njima se mogu prilagođavati kamere, prikazati selektivno, a ovisno o veličini monitora se povećavaju mogućnosti kvalitetnijeg prikaza i rezolucije slike.

Uređaji za obradu video slike se dijele na analogne i digitalne. Analogni ima sekvencijalni prijenosnik koji signal s više kamera prebacuje jedan za drugim. To znači da se slike prebacuju jedna za drugom u određenom vremenskom razmaku, a imaju detektore koji u slučaju izmjene parametara automatski prebacuje prikaz na kameru s anomalijom. Digitalni mogu biti *quad* djelitelji, video multiplekseri i video detektori pokreta. *Quad* omogućava istovremeni prikaz više video signala na monitoru, najčešće četiri. Multiplekseri funkcioniraju tako da video preklopnici u vrlo kratkom roku mogu proslijediti signal video rekorderu na snimanje, dok više signalni prikaz nastavlja prikazivati sliku u stvarnom vremenu na monitoru. Video detektor pokreta analizira ulazni signal s izvora, te ako je došlo do pomaka u njegovom parametru, on pobuđuje alarm.

Mediji za prijenos podataka su vodiči koji prenose video signal od kamere do monitora. Mogu biti žičani (koaksijalni, telefonski, optički i drugi kablovi) i bežični (mikrovalni i infracrveni prijenos, te raznim frekvencijama).

Uređaji za analogno i digitalno snimanje služe za pohranu video zapisa. Gotovo je nezamislivo da danas postoji analogni sustav s videorekorderima za pohranu zapisa na kasetama, barem ne u financijskim institucijama. Zamijenili su ih digitalni koji imaju mogućnost pohrane podataka na diskovima velikih kapaciteta, većinom diskovi s nekoliko desetaka terabajta podatkovnog prostora.

Pomoćni uređaji služe kako bi nam pojednostavili i olakšali rad sustava, a mogu biti razni reflektori za noćno snimanje, upravljačke tipkovnice, pojačivači signala i slični uređaji. [14]

9. TJELESNA ZAŠTITA

Tjelesna zaštita koja se koristi u bankama i financijskim institucijama koje su posebno štićeni objekti, imaju posebne uvjete koje moraju ispunjavati kako bi se ostvarili svi uvjeti tjelesne zaštite držeći se zakona[35] i pravilnika[36], a uvjeti su slijedeći:

- obavezna izrada procjene ugroženosti objekta, procjena stvarnog stanja, analiza mogućih ugroza i mjera tjelesne zaštite
- izrada kategorizacije objekta prema procjeni ugroženosti
- određivanje modela zaštite
- izrada elaborata koji određuje zadatke i postupke zaštitara u slučaju ugroze
- određivanje dužnosti zaštitara u vremenskom periodu kad se vrši primopredaja vrijednosti
- određivanje hodograma i postupaka ponašanja zaštitara ili zaštitara specijalista u slučaju aktivacije alarmnog sustava
- izrađivanje uputa za zaštitare koji se nalaze u objektu i elaborirati njihove dužnosti na radnom mjestu
- izrađivanje hodograma aktivnosti elaboratom, ulaske i izlaske zaposlenika, stranaka, transport novca i vrijednosti, predaju smjena itd.
- izrađivanje naputaka za postupanje u slučaju ugroze.

U procjeni ugroženosti odredit će se kategorizacija objekta, a to su sljedeće tri kategorije:

Prva kategorija su objekti koji su:

- glavne zgrade banke
- distribucijski centri za novac
- zgrade s glavnim serverima i arhivom
- svi ostali objekti koji su procijenjeni u 1. kategoriji ugroženosti.

Model zaštite:

[35] Zakon o privatnoj zaštiti (Narodne novine, 16/20)
[36] Pravilnika o uvjetima i načinu provedbe tjelesne zaštite (Narodne novine 45/2005)

- izraditi protokole za ulaze u banku, prilaz vozila, glavni ulaz, ulaz za službenike…
- obavezno osigurati minimalno četiri zaštitara po smjeni
- odrediti sustav tehničke zaštite, kontrola prolaska, sustav protuprepada, video nadzora, protuprovale i CDS
- organizacija plana ophodne tjelesne zaštite, ophodnju obavljaju najmanje dva zaštitar
- restrikcija neregistriranog ulaska službenika u objekt
- vođenje evidencije i utvrđivanja identiteta stranke
- minimalno jedan zaštitar u sali s šalterima
- angažirati privatnog detektiva radi provjere učinkovitosti sustava.

Druga kategorija su prostori u kojima je protok novca manji nego u prvoj kategoriji, te su manje kompleksni za zaštitu.

Model zaštite:

- izraditi protokole za ulaze u banku, prilaz vozila, glavni ulaz, ulaz za službenike…
- osigurati minimalno tri zaštitara po smjeni
- odrediti sustav tehničke zaštite, kontrola prolaska, protuprepadni sustav i video nadzor
- organizacija plana tjelesne zaštite, ophodnju obavlja minimalno jedan zaštitar
- restrikcija neregistriranog ulaska službenika u objekt
- vođenje evidencije i utvrđivanja identiteta stranke
- zaštitar svakih sat vremena mora obilaziti šaltersku prostoriju
- angažirati privatnog detektiva radi provjere učinkovitosti sustava.

Treća kategorija su prostori koji ne zadovoljavaju prvu ili drugu kategoriju.

Model zaštite:

- izraditi protokole za ulaze u banku, prilaz vozila, glavni ulaz, ulaz za službenike…
- osigurati minimalno jednog zaštitara po smjeni

- odrediti sustav tehničke zaštite, protuprepadni sustav i video nadzor
- ophodnja se provodi po potrebi
- vođenje evidencije i utvrđivanja identiteta stranke
- šalterski prostor obilazi jednom u dva sata. [13]

9.2. Zaštitarska služba štićenih objekata

Svaka pravna osoba koja otvara vrstu djelatnosti koja se bavi financijama, manipulacijom novca, vrijednosti i slično, mora ispunjavati neke od uvjeta osiguranja i zaštite, u ovom slučaju govorit će se o unutarnjoj tjelesnoj zaštiti odnosno zaštitarskoj službi. Svaka pravna osoba, ima mogućnost da osnuje vlastitu unutarnju službu osiguranja prema svim propisima RH, ili u drugom slučaju da koristi usluge vanjske firme (profesionalna zaštitarska tvrtka koja ima ovlasti i licence izdane od RH).

Svaka od tih navedenih opcija zaštite ima svoje prednosti. Ako se uzme u obzir solucija vlastite službe za sigurnost, postoji mogućnost smanjenja troškova. Gledajući u obzir drugu opciju, unajmljivanje vanjske profesionalne zaštitarske tvrtke ima nešto više prednosti. Možda će troškovi biti veći nego s prvom opcijom, ali će se prvo prebaciti odgovornost tjelesne zaštite na unajmljenu tvrtku. Nadalje je u startu bolja prednost zbog bolje stručnosti profesionalnog osoblja, te se ne treba brinuti o rasporedu i organizaciji smjena i broja zaštitara. Osim što nude usluge tjelesne zaštite, iste tvrtke mogu ponuditi usluge i tehničke zaštite, osposobljenost rada vlastitog osoblja na vlastitim sigurnosnim sustavima.

Pravna osoba u vlasništvu financijske ustanove ima pravo osnivati vlastitu zaštitarsku službu, koja mora ispunjavati slijedeće uvjete:

- ima vlastite prostore namijenjene za zaštitarsku službu usklađene sukladno propisima o posebnim prostornim i tehničkim uvjetima za smještaj oružja, zaštitu od požara, krađa itd.
- zaposlenici zaštitarske službe ispunjavaju sve zakonske obaveze RH.

Osoba koja ispunjava slijedeće uvjete, ima pravo obavljanja poslova tjelesne zaštite:

- mora biti državljanin RH s prebivalištem u RH

- mora imati najmanje 18 navršenih godina
- mora ispunjavati posebne fizičke i psihološke uvjete koje se utvrđuju na liječničkom pregledu
- posjedovanje minimalno srednje stručne spreme
- mora imati položen stručni ispit Ministarstva Unutarnjih poslova RH.

Za vrijeme obavljanja dužnosti, zaštitar ima slijedeće ovlasti:

- utvrditi identitet stranke koja ulazi u objekt
- zapovjediti osobi koja remeti red i mir unutar objekta, da napusti isti
- zabraniti kretanje osoba u neovlaštenom području
- zadržati osobu unutar objekta i dočekati s njom policiju i izručiti ju policiji, ukoliko je osoba počinila kazneno djelo ili prekršaj
- pregledati osobu ili vozilo prilikom ulaska u objekt.

Zaštitaru je dozvoljena uporaba sile samo u slučaju ako na drugi način ne može spriječiti:

- napad osobe koji ugrožava njegov život ili osoba koje štiti
- napad osobe s ciljem uništavanja vrijednosti.

Zaštitari su ovlašteni nositi kratko vatreno oružje koje smiju koristiti samo ako ni u kojem drugom slučaju ne mogu spriječiti napad koji ugrožava živote ili uništava vrijednosnu imovinu. Prije upotrebe vatrenog oružja, zaštitar mora dati upozorenje napadaču da će upotrijebiti isto te ispucati u zrak hitce upozorenja. Zaštitar je dužan voditi računa o sigurnosti osoba koje se nalaze u blizini uporabe vatrenog oružja.[21]

10. ZAŠTITA VRIJEDNOSTI U TRANSPORTU

Profesionalne zaštitarske tvrtke ili unutarnje zaštitarske službe moraju posjedovati odobrenje prema Zakonu o privatnoj zaštiti[37], ukoliko štite i obavljaju transport novca. Prijenos novca obavlja se na slijedeći način: da se novac pohranjuje u posebne spremnike (kofere) koji su opremljeni elektrokemijskom zaštitom, koja u slučaju pokušaja obijanja ili nasilnog otvaranja spremnika, aktivira sustav koji označava i uništava novac. Ti spremnici za pohranu novca se transportiraju u specijalnim transportnim vozilima.

Uvjeti koje mora posjedovati vozilo za transport novca:

- oklopljena kabina za posadu, minimalnu protubalističku razinu zaštite (FB3/BR3<NS>[38]), te cijelo vozilo može biti oklopljeno, kabina s razinom zaštite FB3/BR3<NS>, a ostatak vozila s manjom razinom zaštite
- protubalistička stakla
- unutar vozila moraju biti dva odijeljena prostora, jedan za posadu i drugi za teret
- transportno vozilo mora imati ugrađenu protuprovalnu zaštitu
- vozilo mora imati oznaku da je novac koji se transportira, zaštićen elektrokemijskom zaštitom
- vozilo mora imati ugrađen GPS sustav
- vozilo mora imati komunikacijski sustav, jedan za komunikaciju posade međusobno i jedan za komunikaciju sa centralom i policijskom postajom
- mora biti opremljeno s najmanje dva vatrogasna aparata, jedan za teretni prostor i jedan za posadu
- u teretnom prostoru mora biti ugrađen sef s oružjem u slučaju napada.

Posadu vozila čine vozač i minimalno jedan zaštitar u pratnji, a svi članovi moraju biti naoružani kratkim vatrenim oružjem i opremljeni neprobojnim prslucima, te komunikacijskim sustavima.

[37] Zakon o privatnoj zaštiti (Narodne novine, 16/20)
[38] FB3/BR3<NS> - normizirana oznaka protubalističke zaštite, ovim certifikatom garantira se zaštita od metaka kalibra do 10mm

Prijevoz novca Hrvatske narodne banke se izvodi u specijalnim balističkim transporterima uz policijsku pratnju.

Zaštita i distribucija novca i vrijednosti inozemnih financijskih institucija i novčarskih tvrtki koji se odvija kroz Republiku Hrvatsku, provode se prema važećim propisima privatne zaštite i zaštite novčarskih institucija Republike Hrvatske. [7]

11. SUSTAV NADZORA ZAŠTITARSKE SLUŽBE

Sustav koji služi za kontrolu terenskog obilaska čuvarske službe, postavlja se na kritične točke, kako bi se povećala efikasnost zaštitara i povećala njihova sigurnost. Osim što se koriste za nadzor zaštitarske službe, također imaju primjenu u praćenju:

- kretanja osoba i materijalnih stvari (najviše je rasprostranjeno u proizvodnim procesima)
- kretnje vozila (službenih i specijalnih vozila)
- razni nadzori (obilazak bankomata i drugih predmeta i objekata koji se nalaze van lokacije).

Sustav za nadzor obilaska čuvarske službe se sastoji od:

- ručnog čitača
- jedinice za ispis podataka
- jedinice za prijenos podataka
- trake s podacima
- naredbovne mape
- mape s natuknicama
- softverske podrške.

Ručni čitač radi na jednostavnom principu u kojem se čitač povlači preko trake s podacima, a u njega se mogu pohraniti podaci zaštitara, njihova povijest obilazaka i natuknice. Beskontaktni su i imaju dug vijek trajanja, te su prilagođeni za sve vremenske uvijete.

Jedinica za ispis podataka služi za ispis podataka koji se nalaze na ručnom čitaču. Daju informacije o vremenima i mjestima obilaska, zaštitarima i njihovim informacija, sažimaju izvještaj obilaska i propuste koji su se dogodili na nenadziranim mjestima.

Jedinica za prijenos podataka se povezuje s računalom, te prenosi podatke s ručnog čitača.

Trake s podacima mogu biti za unutarnju ili vanjsku montažu gdje se može očekivati slučaj razbojništva. U trake se unosi kod, koji je neizbrisiv i nije ga moguće kopirati.

Naredbovna mapa prati sve aktivnosti sustava za nadzor čuvarske službe, ne zahtjeva računalnu podršku i programe. Promjene je moguće izvesti samo pomoću jedinice za prijenos podataka.

Mapa s natuknicama sadrži 20 programiranih traka s posebnim natuknicama. Kada se uoči neka nepravilnost na mjestu, unosi se pomoću čitača na traku i automatski se memorira nepravilnost toga mjesta.

Softverska podrška omogućuje računalno praćenje svih statistika, parametara, informacija i nepravilnosti vezano za kontrolne točke koje obilaze zaštitari. Sve informacije se skupljaju na jedno mjesto, koje prikazuje podatke kompletnog sustava. [14]

12. *CYBER* KRIMINAL I ZAŠTITA OD *CYBER* NAPADA

Budući da živimo u digitalnom dobu, svjetska ekonomija se digitalizirala, kupovinu obavljamo internetskim putem, koristimo internet bankarstvo i ostale financijske transakcije i usluge. Kako raste internet trgovina i bankarstvo, tako raste i internet kriminal. Kako se internet bankarstvom prebacuje sve više novaca, tako je uzročno posljedična reakcija internet otuđivanje. Budući da banke više ne drže velike novce u sefovima, pljačke banaka se ne „isplate“, tako da se većina kriminala prebacila online. Najčešća metoda *cyber* kriminala je *phishing* metoda, čiji je princip slanja lažnih elektroničkih poruka korisnicima, kako bi im otkrili osobne podatke. Uz ove metode, vrlo učinkovita metoda napada je pomoću zlođudnih programa, npr. metodom trojanskog konja. Ova metoda napada se temelji na ubacivanju zlođudnog programa na računalo ili pametni telefon žrtve, koja obavlja transakcije i kupovinu. Ovisno o svojoj složenosti, ti trojanski konji, mogu pratiti zaslon računala i rad tipkovnice, a koriste se da uhvate IP adresu korisnika. Banke se pokušavaju zaštiti korištenjem virtualnih tipkovnica (funkcionira na principu da se na zaslonu pojavi zaslonu tipkovnica na kojoj je numerički prikaz, na koji se klikom miša ili dodirom na ekran unosi PIN). Međutim, hakeri pomoću snimanja zaslona računala žrtve, „zaobilaze“ fizičku tipkovnicu i tako saznaju PIN.

Neka od metoda zaštite pojedinca od *cyber* napada:

- izbjegavanje otvaranja sumnjivih poveznica, stranica, e-pošte itd.
- korištenje *spam* foldera
- upotreba antivirusnih programa i vatrozida
- upotreba antivirusnih programa s najnovijom verzijom ažuriranja
- obavezno izbjegavanje antivirusnih programa s ilegalnih stranica (*torenti*)
- redovna provjera elektroničkog računa
- upotpunjavanje znanja o online zaštiti.

Vrste *cyber* prijetnji financijskim institucijama online programima:

1. *Keylogger* – program koji prati unos na tipkovnici. Program prati i bilježi unos žrtve na tipkovnici prilikom unošenja, pohranjuje taj unos, a kasnije napadač ulazi u prostor gdje su pohranjeni podatci unosa i koristi se njima. Napadači se koriste programima

koji se aktiviraju nakon unosa ključnih riječi, te snimaju zaslon ekrana ili memoriranjem PIN-a prilikom unosa na fizičkoj tipkovnici.

2. Trojanski konj – zloćudni program koji korisnici preuzmu i instaliraju na vlastito računalo ili pametni uređaj. Većinom su to na lažne nagradne igre, razne virtualne igrice i slični sadržaji. Program funkcionira tako da kad ga žrtva preuzme, omogućuje se istom pristup na računalu, koji preuzima njegove funkcije i kompletnu kontrolu nad njegovim radom. Trojanskog konja (program) naprave stručnjaci za računala i računalne programe ili ga napadač nađe na crnom tržištu i otkupi od drugog napadača (haker). Bankarski trojanski konji su specifični programi kojima je osnovna namjena napad na bankarske sustave ili na druge digitalne ekonomske sustave koje online upravljaju novcem i vrijednosnicama. Ovakva vrsta napada temelji se na krađi osobnih podataka, identiteta i PIN-ova korisnika banaka, te preuzimanju kontrole nad računalom. Trenutno ne postoji stopostotna zaštita od bankarskih trojanskih programa, ali se tvrtke za izradu antivirusnih programa svakodnevno bore kako bi omogućili potpunu zaštitu svojim korisnicima. Računalne viruse izrađuje posebna grupa profesionalnih *cyber* kriminalaca. Bankarski „trojanac“ je programiran tako da filtrira podatke od njemu posebne važnosti, to jest, kada korisnik pristupi internet bankarstvu, aktivira tog trojanskog konja koji počne prikupljati podatke. Oni presreću podatke, odnosno pinove korisnika prilikom unošenja i te podatke šalju napadaču koji onda dobije pristup žrtvinom računu i nakon toga si prebacuje novac na svoj račun koji nema mogućnost nadziranja.

3. Otimanje sjednica[39] – ovo je zapravo jedan oblik trojanskog konja, koji se ubacuje u autenticiranu sjednicu. U ovoj vrsti napada, zloćudni program mijenja sadržaj transakcija, gdje korisnik X prebacuje neku količinu novaca korisniku Y, napadač se ubacuje u sjednicu u kojoj može promijeniti iznos novaca i prebaciti na račun kojim on upravlja, a osim toga napadač može unijeti i novi nalog za transfer novca. Naravno, napadač koristi zaštićeni račun koji se ne može pratiti. [22]

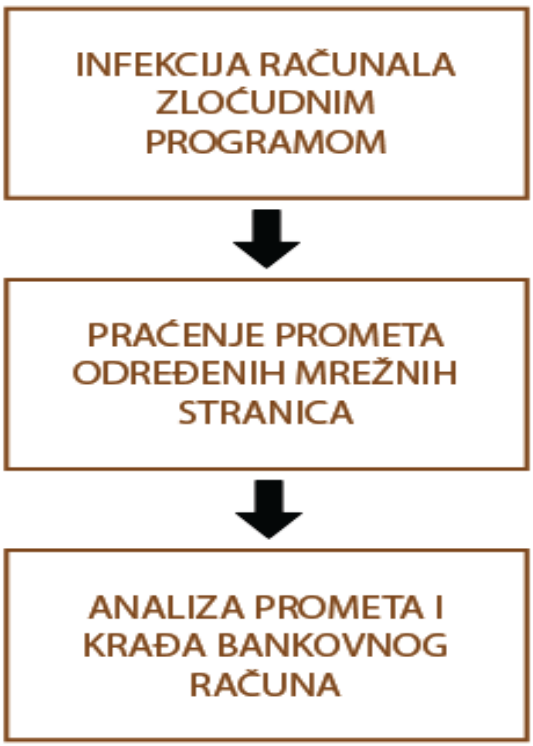
4. *Form grabbing* – ovo je metoda kojom se napadači koriste da bi preuzeli kontrolu podataka s prozora na računalu ili pametnom telefonu. Napadač presreće podatke

[39] Sjednica – veza između korisničkog računala i računala poslužitelja.

kada korisnik bankovnih aplikacija upisuje svoje podatke u neki obrazac prilikom internet kupovine. Na primjer, prilikom ispunjavanja podataka bankovnih računa, brojeva kartica, pinova i slično. Ovakvi zlćudni programi prikazuju na web pregledniku identičnu stranicu kao na pravoj. Međutim na provjerenim verificiranim stranicama se ne traži od korisnika PIN, dok zlćudni program to traži od korisnika. Kada ga korisnik upiše, napadač dobije podatke koji mu trebaju i onda ima pristup žrtvinom online bankarstvu.

5. *Pharming* – napadač kreira internet stranicu koja izgleda kao stranica banke koja iskoči korisniku prilikom pristupa internet bankarstvu. Takva stranica mijenja sadržaj prometa između banke i korisnikovog internet preglednika. Postoji nekoliko tehnika trojanskog konja koji vrši *pharming*, a jedna od njih je kad se isti instalira na računalo korisnika, izradi svoj certifikat i tako zaobiđe pojavu upozorenja o mogućoj prijetnji.

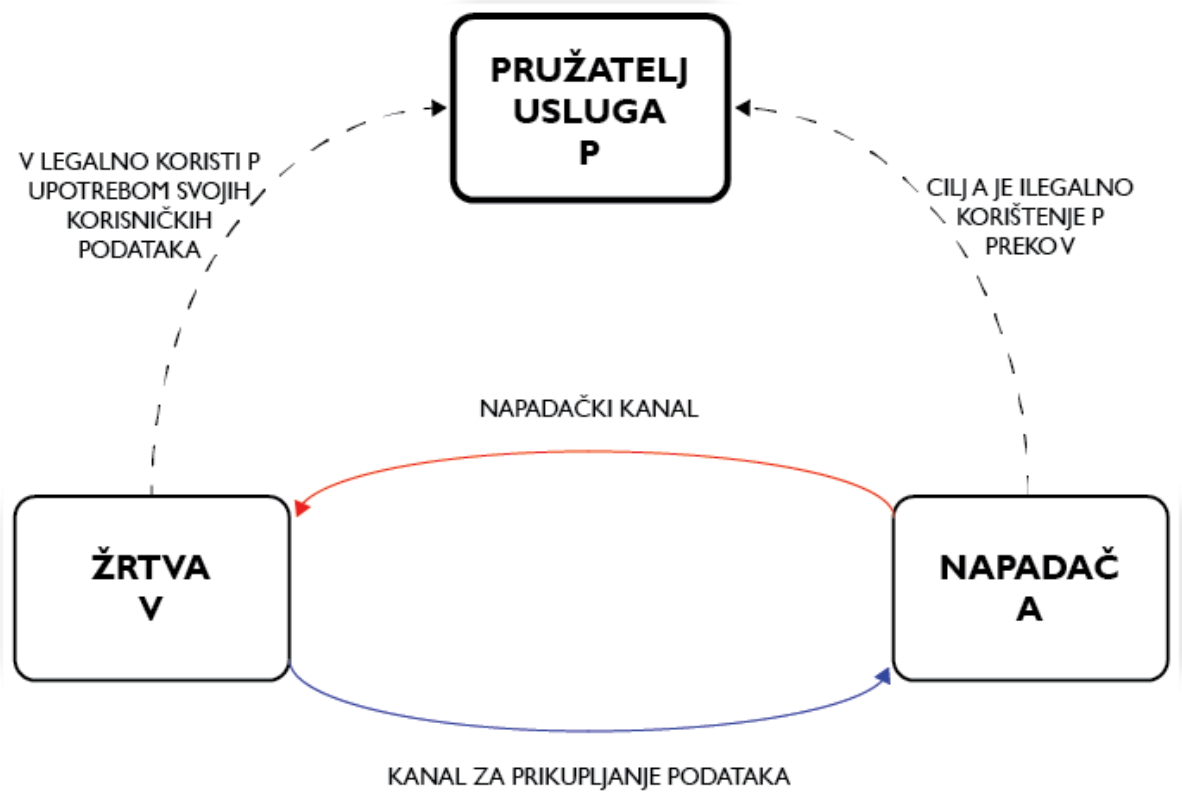
6. Zlćudni programi u više koraka – prvi korak je infekcija računala, gdje se zlćudni program instalira na korisnikovo računalo. U drugom koraku se prati kriptirani program mrežnih stranica i te podatke program šalje napadaču. U trećem koraku napadač prati podatke žrtve i prilikom pristupanja bankovnom računu presreće podatke na tipkovnici.



Slika 5. Tok izvođenja napada [23]

7. Lažno predstavljanje – u ovoj metodi se koriste slijedeći akteri:

- banka
- korisnik
- napadač.



Slika 6. Napad lažnim predstavljanjem [23]

Banka svakome korisniku svojih usluga daje korisnički profil (njegov korisnički račun i lozinku) za pristupanje svom računu. Napadačev je cilj otuđiti korisnikove podatke za pristupanje računu, odnosno predstaviti se banci da je on korisnik. Međutim, napadač može i promijeniti politiku presretanja podataka, te se korisniku lažno predstavit kao davatelj usluga (banka), koja je u stvari ista metoda kao i kod pokušaja lažnog predstavljanja banci. Naime, napadač od korisnika lažnim predstavljanjem uzima njegove podatke i tako ima slobodan pristup njegovom računu. Neke od metoda lažnog predstavljanja su *phishing* i lažno predstavljanje *keyloggerima*.

8. Trojanski konji „obitelji“ – trojanske konje možemo svrstati u neke obitelji:

8.1. Limbo/Nethell – koriste metodu *phishinga* i zlonamjernih internet stranica. Napadač žrtvu namami na zaražene internet stranice, koje ubacuju virus u obliku internet *plugina*, te tako dok se nalazi na računalu, prati podatke korisnika (kolačići) i koristi ih za svoje svrhe.

8.2. ZeuS/Zbot/Wsnpoem – koriste elektroničku poštu s neželjenim sadržajem, gdje mame korisnika da ih otvori i tako se instaliraju na računalo, a za razliku od Limbo/Nethella kada se jednom instaliraju na računalo, sakrivaju svoju prisutnost. Ulaze u internet preglednik korisnika, prikupljaju podatke o prometu i kolačiće te tako dolaze do željenih podataka. [23]

Godine 2020. izvršen je veliki *cyber* napad na mađarske telekomunikacije i banke. Radilo se o napadima na DDoS[40] (napad uskraćivanja resursa), u kojem su napadači iz Rusije Kine i Vijetnama, iskoristili veliku količinu podataka mreže, ubacili se u nju, unijeli velike količine podatkovnog prometa i na taj način ju paralizirali. Prema nekim podatcima, prijenos podataka bio je 10 puta veći od onoga koji je sustav mogao podnijeti. Prema podatcima iz telekomunikacijske tvrtke Magyar Telekom, to je bio jedan od najvećih *cyber* napada u Mađarskoj. Magyar Telekom se djelomično uspio obraniti od napada, međutim u glavnom gradu, Budimpešti, se dogodio propust. Napad ruskih, kineskih i vijetnamskih hakera dogodio se u nekoliko valova, te poremetio neke od bankarskih sustava u cijeloj državi, između ostalih i mađarske OTP banke. [25]

U 2020. godini dogodio se veliki porast *cyber* napada, kako na financijske institucije, tako i na ostale servise koje obavljaju digitalni oblik bankarstva. Posebno su povećani DDoS napadi.

Australske banke su također 2020. godine zabilježile porast *cyber* kriminala. Naime u tom napadu su napadači (prema nekim tvrdnjama i javnim priznanjima, australska organizacija hakera The Silence Hacking Crew preuzela je odgovornost za napad),

[40] DDos (Distributed Denial of Service) – napad uskraćivanjem resursa, kada se preopterećuje računalna mreža slanjem višestrukih zahtjeva poslužitelju i tako se zaustavi promet.

poslali elektroničku poštu financijskim institucijama, u kojoj traže otkupninu u obliku Monero[41] kriptovalute. [26]

Mnogi stručnjaci pokušavaju skrenuti pozornost na DDoS napade i njihovu učestalost, te njihovo korištenje u širenju *ransomware*-a (ucjenjivački softver). *Ransomware* je zloćudni softver koji žrtvi onemogući pristup računalu, potom napadač od žrtve kojoj je zaplijenio pristup računalu, traži uplatu određene svote novca kako bi ponovno omogućio pristup računalu.

U posljednje vrijeme *ransomware* napadi su najviše zabilježeni na smartphone uređajima, u kojima dobiju pristup datotekama i preglednicima.

Treba naglasiti jedan od najvećih pokušaja *cyber* napada, točnije DDoS napada u veljači 2020. godine na AWS (Amazon web service), koji je pokušao ubaciti veliku količinu podataka. Prema njihovim podatcima to je bio protok podataka od 2,3 terabajta u sekundi, što je za 44% veća količina podataka od zadnjeg najvećeg pokušaja napada. [27]

[41] Monero – digitalna kriptovaluta koja nudi visoku razinu anonimnosti korisnicima i njihovim transakcijama.

13. *CYBER* SIGURNOST FINANCIJSKIH INSTITUCIJA

Cyber sigurnost je mjera sigurnosti zamišljena kako bi se u financijskom sektoru obranila banka (poslužitelj usluga), korisnik i njegovo računalo, mreža i informacijski podatci u digitalnom obliku, od neovlaštenih upada u same bankovne sustave, računala i podatke korisnika, napada na financijsku, informacijsku i osobnu sigurnost, te možebitno uništavanje ili krađa istih. Cilj je za zaštiti vlastite povjerljive informacije o poslovanju, financije, intelektualno vlasništvo i na kraju samu reputaciju.

Informacijska i bankovna sigurnost je od velike važnosti i interesa svake države, tako da svaka država mora razviti strateški plan za obranu. Primjer studije [24] Nacionalnog centra za *cyber* sigurnost[42] u Ujedinjenom Kraljevstvu 2017. godine, u kojoj se pokazuje da su istraživanjem došli do podataka kako je više od 50% britanskih tvrtki bilo žrtva nekog oblika *cyber* napada. Iz tog razloga, vlada UK odlučila je financijski pomoći tvrtkama da podignu svoju sigurnost i obranu od *cyber* napada.

Financijske institucije posjeduju vrlo važne podatke i informacije o poslovanju te informacije o svojim korisnicima. Osim toga, glavna i najvažnija stavka financijskih institucija su sredstva kojima ona raspolaže, velike količine novca i vrijednosti, koje su *cyber* kriminalcima glavna meta. *Cyber* napadači posjeduju velika znanja o računalnim tehnologijama koja koriste kako bi upali u tok financijskih sustava i tako se ilegalno okoristili informacijama i novčanim sredstvima.

Napad na bankarski sustav smatra se najvećim napadom jer može ukrasti, izbrisati i izmijeniti podatke. Digitalna tehnologija ima velik utjecaj na bankarski sustav, budući da banke i općenito financijske institucije ovise o trećoj strani. Koriste resurse drugih firmi koje izrađuju programe za digitalne transakcije i internet bankarstvo, jer financijske institucije kao takve nemaju stručni kadar koji se bavi sustavima za izradu programa, te zaštitu i sigurnost aplikacija. Iako banke i institucije uvelike ulažu svoje napore kako bi unaprijedili tehnologiju, teško da mogu pratiti korak s informacijskom tehnologijom, te tako ovise o vanjskim rješenjima. Istraživanje Richarda

[42] Nacionalni centar za *cyber* sigurnost – osnovan 2016. godine u Ujedinjenom kraljevstvu. Bavi se informiranjem privatnih i javnih sektora o računalnoj sigurnosti.

Summerfielda[43] (2014.) navodi kako je 50 mrežnih stranica poznatih bankovnih sustava bilo napadnuto i tako stvorilo gubitak veći od jedne milijarde američkih dolara na godišnjoj razini. [44]

Bankarski sektor pokušava pratiti informatičke inovacije i pratiti korak s tehnologijama koje se odnose na pravilnike i nove propise koje postavljaju međunarodne institucije. Uz dvije metode autentifikacije, pokušavaju se spriječiti razni cyber napadi posebno na račune korisnika. Jedna metoda autentifikacije je metoda slanja jednokratnih kodova unutar aplikacije, koja funkcionira tako da kada korisnik obavlja online kupovinu, upisuje sve podatke kartice na stranici koja je zaštićena te nakon tog koraka banka unutar aplikacije za online bankarstvo šalje korisniku jednokratni kod koji upisuje na stranici prilikom odobravanja kupovine. Tako se pokušava jednokratnim kodovima spriječiti daljnje korištenje ukoliko napadač već posjeduje neke podatke od korisnika. Ova vrsta autentifikacije se pokazala vrlo učinkovitom. Međutim, još uvijek postoje bankarske institucije koje u svom online poslovanju i aplikacijama ne koriste dvostruku autentifikaciju. Postoji slučaj u jednoj od banaka u kojoj je napadački softver napao neke od korisničkih računala, u kojem je isti softver imao funkciju zaobilaženja kontrole i mogao je slobodno koristiti žrtvin račun za transakcije. Kako bi napadači izbjegli sumnjivost, nisu radili velike iznose transakcija koji bi bili očiti, nego su koristili manje iznose i tako sistemom sporog „kapanja“ radili novčane transakcije. Sjedinjene Američke Države imaju pisani zakon, koji nalaže da u slučaju krađe, banka u kojoj korisnik ima račun, ukoliko je netko neovlašteno izvršio otuđivanje sredstava, mora korisniku vratiti puni iznos ukradenih sredstava. Vlasnik računa treba prijaviti krađu unutar 60 dana od dana neovlaštene transakcije.

U *online* članku The Telegrapha [45] od 14. kolovoza 2017. godine usporedili su se *cyber* napadi iz 2016. i 2015. godine te je dobiven zaključak kako je u odnosu na 2015. godinu *cyber* napad porastao 122% u odnosu na 2016. godinu. Zabilježen je gubitak od 10,5 milijardi američkih dolara, a internet transakcije porasle su za 10%.

[43] Članak u listu Financier Worldwide, autora Richarda Summerfielda govori o važnosti ulaganja novčanih sredstava s ciljem zaštite od *cyber* napada na financijski sektor, ulaganjem u tehnologiju i pokušaja držanja koraka ispred cyber napadača.

S ciljem osiguranja online sigurnosti, Europska unija i nacionalni institut za standarde, uspostavili su pet faktora za digitalnu online zaštitu:

- Identifikacija – organizacija i razumijevanje kako bi se pravovremeno zaštitili i spriječili nepotrebne rizike
- Zaštita – organiziranje zaštitnih mjera kako bi ograničili moguće prijetnje
- Detekcija – provođenje koraka identificiranja *cyber* sigurnosti
- Reakcija – poduzimanje mjera nakon identifikacije problema
- Oporavak – planiranje mjera za povraćanje ugroženih podataka.

Na ciljeve politike potrebno je paziti. Prvo, svi ciljevi politike *cyber* sigurnosti trebaju biti jasno objašnjeni, a drugo, politika se treba bazirati na poboljšanju i potencijalnoj koristi, a ne na gubitak. Treće, ciljeve treba posložiti po prioritetima u pogledu sigurnosti financijskog sektora i njihovim rizicima. Jedna od presudnih tehnika postizanja *cyber* sigurnosti je učestalo ažuriranje aplikacija. [24]

14. GDPR (GENERAL DANA PROTECTION REGULACIJA)

Opća odredba o zaštiti podataka EU 2016/659 donesena je 2016. godine i usvojila ju je Europska unija, a stupila je na snagu 2018. godine, kojim je završeno prijelazno razdoblje od dvije godine. Njome se regulira zaštita podataka i zaštita privatnih podataka osoba, stanovnika Europske unije.

Svaka organizacija koja prikuplja, obrađuje i koristi privatne podatke mora se pridržavati ove regulative i usvojiti ju. Jedino područje koje je izuzeto iz GDPR-a su podatci osoba protiv kojih se vode kriminalni postupci i izvanredni sustavi zaštite.

Svaka država članica EU mora imenovati regulatorno nadzorno tijelo, koje pomaže u usklađivanju. Problem se pojavljuje u razumijevanju i tumačenju zakona, kako Europska unija ima veliki broj članova, svaka od njih usvaja taj zakon, ali je moguće da će ga drugačije protumačiti i provoditi.

EDPB (europski odbor za zaštitu podataka) je neovisno tijelo europske unije koje ima potpuni pravni status i odgovoran je za nadzor primjene pravne regulative GDPR-a te će biti odgovoran za rješavanje svih sporova nastalih između nadzornih tijela.

GDPR će se provoditi tamo gdje su podatci automatski obrađeni, nalaze se u automatiziranim sustavima za obradu podataka ili u sustavu u kojem je djelomična obrada podataka, ali taj sustav ga formira u cjelinu ili djelomično. Propis regulira od čega se sastoje podatci (identifikacijski brojevi, internet identifikatori kao što su IP adrese, podatci o lokaciji i ostali podatci koji se odnose na praćenje ponašanja pojedinca).

Direktive vezano za ovu pravnu odredbu se ne odnosi samo na organizacije unutar EU, već i za:

- organizacije sa sjedištem unutar EU, bez obzira vrši li se obrada podataka u istoj ili izvan nje
- organizacije izvan EU, koje obavljaju razmjenu robe unutar EU, posluju i imaju određene poslovne aktivnosti unutar EU.

Značajne promjene GDPR-a:

- primjena načela privatnosti principom „dizajna privatnosti“ i njegovog implementiranja u nove tehnologije i inovacije
- provođenje procjene utjecaja vanjskih faktora na privatnost
- prava na prijenos podataka i pravo na brisanje i zaborav podataka
- zahtjev za zaštitom podataka u slučaju povrede prava privatnosti
- globe za kršenje prava u vrijednosti od 20.000.000 eura ili 4% od godišnjeg prometa organizacije
- posebne uredbe i prava za zaštitu podataka djece i maloljetnika.

Principi transparentnosti zahtijevaju da je informacija i radnja vezana za procesuiranje podataka jednostavna za razumijevanje, jasna i smislena.

Sve informacije o osobi, koje na bilo koji način mogu neku osobu identificirati (direktno ili indirektno) preko informacija dobivenih o njoj, smatraju se osobnim podatcima. Tako omogućujemo osobnim podatcima, imenu, prezimenu, osobnom identifikacijskom broju, podatcima o lokaciji, online identifikatorima i ostalim podatcima da se konstantno prikupljaju obrađuju i ažuriraju, te sustavi i programi mogu pratiti stalni napredak tehnologije.

Biometrijski podatci su osobni podatci osobe dobiveni posebnim tehničkim obradama koje se odnose na fizičke, fiziološke ili karakteristike ponašanja fizičke osobe, koja omogućuje pristup svojim identifikacijskim informacijama (biometrijski podatci otiska prsta ili slika lica, npr. otključavanje zaslona pametnog telefona otiskom prsta ili slikom lica). Profiliranje može biti bilo koja verzija automatske obrade podataka.

Prava o podatcima korisnika:

- pravo na kopiju podataka
- pravo na brisanje podataka, podatci zahtijevaju od kontrolora da obriše osobne podatke i da se iste više ne može obrađivati
- pravo na prigovor obrade podataka, korisnik ima pravo dati svoju primjedbu na obradu podataka, profiliranje, istraživanje…
- pravo na prenosivost podataka, korisnik ima pravo na zahtjev da mu se omogući da dobije podatke u formatu koje može koristiti na drugom uređaju

GDPR-ovim pravilnikom se zahtjeva od organizacije koja upravlja podatcima, da u slučaju kršenja osobnih prava korisnika, obavezno obavijesti nadležno tijelo.

Obavijest mora sadržavati:

- objasniti postupak kršenja osobnih podataka
- navesti broj korisnika koje su oštećeni kršenjem osobnih podataka
- navesti posljedice kršenja osobnih podataka
- opisati poduzete mjere u slučaju kršenja osobnih podataka ili predložiti mjere koje treba poduzeti.

Svako narušavanje sigurnosti koje dovodi do uništenja, gubitka, oštećenja, promjena, neovlaštenih pristupa ili neovlaštenog otkrivanja podataka smatra se kršenjem osobnih podataka. Oštećeni individualci moraju biti pravovremeno obaviješteni u slučaju visokog rizika koji bi mogao povrijediti njihova prava i slobodu. Kršenja prava osobnih podataka moraju u roku 72 sata od saznanja da su njihova prava oštećena, biti prijavljeni povjereniku za zaštitu podataka. U posebnim slučajevima, kontrolor bi trebao navesti podatke subjekta koje su zahvaćene kršenjem, kako bi ista kontrola mogla reagirati pravovremeno u toj situaciji, proučiti to kršenje podataka i dobili saznanja kako se u budućnosti nositi sa sličnim slučajevima kršenja prava o osobnim podatcima korisnika. [30]

15. ZAKLJUČAK

Ovim radom prikazane su financijske institucije kao meta potencijalnih napada. Bazirajući se na važećim zakonima i propisima RH, ovim se radom pokušalo izvući najvažnije iz pravne regulative, objasniti najvažnije pojmove i sažeti te primijeniti na temu rada. Financijske institucije i novac kroz povijest su prošli velike promjene. Novac kao sredstvo plaćanja i vrijednosni predmet razvio se od kitovih zubi, vrijednosti u obliku alata, sve do donedavne pojave kriptovaluta, koje ustvari vlade država još uvijek nisu priznale kao pravi novac, ali ga je moguće zamijeniti za novac.

Kaznenim zakonom[44] i zakonom o zaštiti novčarskih institucija[45], dva temeljna pravna akta ovog rada, objasnilo se najvažnije u razumijevanju osnovnih pojmova. Kazneni zakon RH objasnio je pojmove krađe, teške krađe, razbojništva, razbojničke krađe i iznude. Zakonom o zaštiti novčarskih institucija objašnjena je podjela kategorija financijskih institucija.

Sustavi tehničke zaštite prikazali su sustave koji su nezaobilazni kada se govori o zaštiti financijskih institucija. Bez kompleksnih procjena ugroženosti objekata i detaljnih analiza mogućih ugroza, nije moguće ni pristupiti postavljanju sustava zaštite objekta.

Služba tjelesne zaštite također je nezaobilazna u štićenju financijskih institucija. Njihove ovlasti i postupanja u određenim situacijama obrađene su i detaljno opisane. Svaka osoba koja obavlja dužnosti tjelesne zaštite mora proći niz psihofizičkih testova i provjera sposobnosti te na kraju položiti stručni ispit, kako bi dobili ovlaštenje za obavljanje istih.

Završni dio rada govori je o *cyber* sigurnosti financijskih institucija, budući da je napretkom tehnologije te online trgovine i poslovanja uvelike premašena brojka u usporedbi s fizičkim plaćanjem. S tim podatkom važno je postaviti najbolje sustave digitalne zaštite kako bi se zaštitili klijenti i same financijske institucije. Za kraj je važno

[44] Kazneni zakon Republike hrvatske (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21)
[45] Zakon o zaštiti novčarskih institucija (NN 56/15, 46/21)

spomenuti da danas veću prijetnju financijskim institucijama predstavljaju hakerski napadi, nego fizičke pljačke banaka.

16. LITERATURA

[1] „Novac kroz povijest“, https://povijest.hr/drustvo/politika/novac-kroz-povijest/ (pregled stranice 23.08.2021.)

[2] „Novac“, https://www.enciklopedija.hr/natuknica.aspx?ID=44191 (pregled stranice 23.08.2021.

[3] „The History of Money in Ten Minutes“, https://www.britannica.com/video/187664/history-money (pregled stranice 23.08.2021.)

[4] A Brief History of Money, https://spectrum.ieee.org/a-brief-history-of-money (pregled stranice 23.08.2021.)

[5] Kazneni zakon Republike hrvatske (Narodne novine, 126/19)

[6] Zakon o zaštiti novčarskih institucija (Narodne novine, 56/15, 46/21)

[7] Zakon o privatnoj zaštiti (Narodne novine, 16/20)

[8] Pravilnik o uvjetima i načinu provedbe tjelesne zaštite (Narodne novine, 45/2005)

[9] Zakon o informacijskoj sigurnosti (Narodne novine, 79/7)

[10] „Krađa“, https://www.enciklopedija.hr/natuknica.aspx?id=33633 (pregled stranice 24.08.2021.)

[11] „Uvod u kriminologiju s osnovama kaznenog prava“, https://www.pravo.unizg.hr/_download/repository/Derencinovic%2C_Davor%3B_Getos%2C_Anna-Maria._Uvod_u_kriminologiju_s_osnovama_kaznenog_prava%5B2%5D.pdf (pregled stranice (24.08.2021.)

[12] „Kaznena djela razbojništva“, http://www.vsrh.hr/CustomPages/Static/HRV/Files/BrkicB_Kaznena-djela-razbojnistva_2002-11_HPR.pdf (pregled stranice 24.08.2021.)

[13] Delišimunović, Davor: Zaštita i sigurnost financijskih institucija, - Zagreb: Tectus d.o.o., (2001.), ISBN: 953-97026-3-1

[14] Delišimunović, Davor: Management zaštite i sigurnosti, - Zagreb: Pragmatekh, (2006.), ISBN: 953-7381-00-5

[15] Delišimunović, Davor: Suvremeni koncepti i uređaji zaštite, -Zagreb: I.T. Graf, (2002.), ISBN: 953-96541-0-6

[16] „Elektronička zaštita artikla od krađe“, https://www.alarmautomatika.com/hr/proizvodi/elektronicka-zastita-artikala-od-kradje/ (pregled stranice 24.08.2021.)

[17] „Cjelovita rješenja zaštite financijskih institucija“, https://www2.alarmautomatika.com/documents/files/promo/bankalog_cro.pdf (pregled stranice 24.08.2021.)

[18] „Banke na meti hakera“, https://zastita.info/hr/casopis/clanak/banke-na-meti-hakera,18717.html (pregled stranice 24.08.2021.)

[19] „Sprječavanje fizičkih napada na ATM uređaje“, https://eucpn.org/sites/default/files/document/files/ATM%20report%20-%20final%20version_HR.pdf (pregled stranice 24.08.2021.)

[20] „Video nadzor – kratka povijest“. https://www.fnikol.mojweb.com.hr/sigurnost/sigurnost/ (pregled stranice 25.08.2021.)

[21] Pravilnik o uvjetima i načinu provedbe tjelesne zaštite (Narodne novine 45/2005)

[22] „Napadi krađom korisničkih sjednica“, https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2007-03-185.pdf (pregled stranice 27.08.2021.)

[23] „Bankarski zloćudni programi“, (https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-02-290.pdf) (pregled stranice 27.08.2021.)

[24] „The significance of cybersecurity system in helping managing risk in banking and financial sector, https://www.researchgate.net/publication/337086201_The_Significance_of_Cybersec

urity_System_in_Helping_Managing_Risk_in_Banking_and_Financial_Sector (pregled stranice 27.08.2021.)

[25] „Mađarske banke i telekomunikacijski operateri pod udarom stranih hakera“, https://www.bug.hr/dogadjaji/madjarske-banke-i-telekomunikacijski-operateri-pod-udarom-stranih-hakera-16737 (pregled stranice 28.08.2021.)

[26] „Silence Hacking Group Threatens Australian Banks of DoS Attacks if Ransom Not Paid“, https://cybersecuritynews.com/hacking-group-australian-organisations/ (pregled stranice 28.08.2021.)

[27] „AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever“, https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/ (pregled stranice 28.08.2021.)

[28] „The Knightsbridge security deposit robbery – almost the perfect crime“, https://www.documentarytube.com/articles/the-knightsbridge-security-deposit-robbery-almost-the-perfect-crime (pregled stranice 28.08.2021.)

[29] „ The great Dunbar armored depot robbery“, https://gilaherald.com/the-great-dunbar-armored-depot-robbery/ (pregled stranice 28.08.2021.)

[30] „Challenges of General Data Protection Regulation (GDPR)“, https://www.researchgate.net/publication/325173474_Challenges_of_General_Data_Protection_Regulation_GDPR (pregled stranice 28.08.2021.)

[31] „Opljačkana banka u Višnjanu“, https://porestina.info/opljackana-banka-u-visnjanu/ (pregled stranice 28.08.2021.)

[32] „Otkrivamo novi oblik zaštite bankomata: Evo što će se dogoditi u slučaju provale“ https://www.vecernji.hr/vijesti/otkrivamo-novi-oblik-zastite-bankomata-evo-sto-ce-se-dogoditi-u-slucaju-provale-1447453 (pregled stranice 30.08.2021.)

[33] Ručno tipkalo, slika 1. u kompilaciji, https://au.rs-online.com/web/p/emergency-stop-push-buttons/7660426/ (pregled stranice 30.08.2021.)

[34] Bežično tipkalo, slika 2. u kompilaciji, https://hogaki.com/wireless-emergency-button-for-our-related-home-alarm-home-security-system-433mhz-panic-button-64344 (pregled stranice 30.08.2021.)

[35] Alarmna nožna šina, slika 3. u kompilaciji, https://www.av-gad.com/product/foot-activated-hold-up-station/ (pregled stranice 30.08.2021.)

[36] Sef s vremenskim kašnjenjem, slika 4. u kompilaciji, https://www.allsafes.ie/img_100_1800_1800_CART1.jpg (pregled stranice 30.08.2021.)

[37] Nagazni tepih, slika 5. u kompilaciji, https://m.media-amazon.com/images/I/71wHHi4+u6L._AC_SS450_.jpg (pregled stranice 30.08.2021.)

[38] Sustav za bežično aktiviranje dimne zavjese, slika 6. u kompilaciji, https://www.smokecloak-residential.co.uk/images/listing_to_details_page_image/medium/pa.jpg (pregled stranice 30.08.2021.)

[39] „BIROSAFE Bulletproof doors,walls and windows“ https://www.asadria.com/en/birosafe-bulletproof-doors-walls-and-windows-en-1522-ecb%E2%80%A2s-certified/ (pregled stranice 30.08.2021.)

[40] „Hrvatski normativni dokument“, https://repozitorij.hzn.hr/norm/HRN+EN+1143-2%3A2014 (pregled stranice 25.11.2021.)

[41] „U ime Republike Hrvatske - presuda“, https://sudovi.hr/sites/default/files/dokumenti/2020-09/12%2012%202012%20FINA.pdf (pregled stranice 25.11.2021.)

[42] „Statistički pregled MUP-a 2015.“ https://mup.gov.hr/UserDocsImages/statistika/2016/Statistika_2015_nova..pdf (pregled stranice 25.11.2021.)

[43] „Cybercrime Surpasses Traditional Crime in the United Kingdom“, https://blog.trendmicro.com/trendlabs-security-intelligence/cybercrime-surpasses-traditional-crime-united-kingdom/ (pregled stranice 25.11.2021.)

[44] „Banking system faces cyber threat“, https://www.financierworldwide.com/banking-system-faces-cyber-threat (pregled stranice 25.11.2021.)

[45] „Cyber attacks on online retailers double in a year as hackers try to steal shoppers' details“, https://www.telegraph.co.uk/news/2017/08/13/cyber-attacks-online-retailers-double-year-hackers-try-steal/ (pregled stranice 25.11.2021.)

17. PRILOZI

17.1. Popis slika