Zaštita zračnih luka od kibernetičkih prijetnji

Jakšić, Dino

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Dino Jakšić

ZAŠTITA ZRAČNIH LUKA OD KIBERNETIČKIH PRIJETNJI

ZAVRŠNI RAD

Zagreb, 2020.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 2. travnja 2020.

Zavod: **Zavod za zračni promet**
Predmet: **Osnove aerodroma**

ZAVRŠNI ZADATAK br. 5845

Pristupnik: **Dino Jakšić (0135242489)**
Studij: Promet
Smjer: Zračni promet

Zadatak: **Zaštita zračnih luka od kibernetičkih prijetnji**

Opis zadatka:

U uvodnom dijelu rada potrebno je izraditi strukturu rada te napraviti pregled dosadašnjih istraživanja u predmetnoj problematici. U narednim poglavljima potrebno je opisati vrste i tipove kibernetičkih prijetnji te njihov utjecaj na zračne luke. Potrebno je opisati preventivne zaštitne mjere koje zračne luke provode u cilju sprečavanja kibernetičkih prijetnji. U posljednjem dijelu završnog rada dati zaključna razmatranja.

Mentor:

dr. sc. Matija Bračić

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

ZAŠTITA ZRAČNIH LUKA OD KIBERNETIČKIH PRIJETNJI

AIRPORT PROTECTION FROM CYBER THREATS

Mentor: dr.sc. Matija Bračić

Student: Dino Jakšić
JMBAG: 0135242489

Zagreb, rujan 2020.

SAŽETAK

U današnje vrijeme internetska tehnologija sve je zastupljenija. Preuzela je glavnu ulogu u našoj svakodnevici, unaprijedila naš život te olakšala svakodnevni posao. S druge strane, s obzirom na njenu zastupljenost javlja se sve veća opasnost od kibernetičkih napada te je potrebno što veću pozornost posvetiti zaštiti i zaštitnim mjerama od napada. Zračne luke jedan su od primjera koji svoje poslovanje zasniva na tehnologiji te su stoga izložene kibernetičkim prijetnjama. Na zračnim lukama postoji osoblje zaduženo za provedbu procesa zaštite. Ono mora biti osposobljeno za pregled putnika, njihove ručne prtljage, predane prtljage te pregled samih zrakoplova. Cjelokupno osoblje dužno je proći zaštitni pregled pri svakom prelasku sa zemaljske na zračnu stranu zračne luke.

Ključne riječi: kibernetički napadi; kibernetičke prijetnje; Internet; tehnologija; zaštita; preventivne mjere i metode

SUMMARY

Internet technology has become a common occurrence in our everyday lives. It improved our quality of life and simplified our daily tasks. However, regarding its growing presence, there is an increase in cyber-attack threats urging us to take notice and improve protection measures. Airports are a technology-based business and they are sensitive to cyber-attacks. Furthermore, within airport there is personnel who perform security measures. After mentioned personnel must be adequately trained so they can be able to perform security check of passengers, their hand-luggage, checked luggage and the aircraft itself. The entire personnel is required to undergo a security check with every crossover from the ground to the air side of the airport.

Keywords: cyber attack; cyber threats; security; Internet; technology; protective measures; airport

SADRŽAJ

1. UVOD

Zračni promet se smatra najsigurnijom vrstom prometa. Unatoč tome, zračne su luke oduvijek bile meta raznovrsnih djela nezakonitog ometanja. Kako bi se takva djela spriječila i kako bi se povećala razina sigurnosti, potrebno je provoditi zaštitne mjere. U glavne elemente zračne luke se ubraja zračna i zemaljska strana.

Zaštita zračnih luka je potrebna kada su u pitanju kibernetički napadi ako se uzmu u obzir opseg različite i osjetljive tehnologije koja se koristi. Ovaj rad opisuje moguće prijetnje, napade od strane *cyber* napadača te zaštitne mjere i metode koje svaka zračna luka mora primijenit kako ne bi došlo do dijela nezakonitog ometanja zračne luke od strane *cyber* napadača.

Svrha ovoga rada je istaknuti važnost zaštite zračne strane zračne luke uz pomoć preventivnih mjera zaštite za sprječavanje kibernetičkih prijetnji.

Rad je koncipiran u šest poglavlja.

Prvo poglavlje prikazuje uvodna razmatranja.

U drugom je poglavlju opisana regulativa u području zaštite zračnog prometa.

Treće poglavlje obuhvaća tipove kibernetičkih prijetnji i napada koji pogađaju zračne luke te zaštitne metode koje je moguće primijeniti.

U četvrtom su poglavlju prikazani primjeri pojedinih kibernetičkih napada.

Peto poglavlje prezentira mjere zaštite koje zračne luke provode u slučaju kibernetičkih napada.

U posljednjem, šestom poglavlju iznesena su zaključna razmatranja.

2. REGULATIVA U PODRUČJU ZAŠTITE ZRAČNOG PROMETA

Najznačajniji element zračnog prometa je zaštita čiji je osnovni zadatak očuvati civilno zrakoplovstvo od djela nezakonitog ometanja. Taj se zadatak ispunjava kombiniranjem mjera s ljudskim i materijalnim resursima. U tom pogledu, potreban je niz pravila o načinu i provedbi zaštite zračnog prometa u svim područjima njegova djelovanja.

2.1. Regulativa tijela Europske unije

Regulativa za europski zračni promet donosi se na razini Europske unije. Europska komisija mjerodavno je tijelo Europske unije za područje zaštite zračnog prometa koje prema potrebama donosi mjere u svrhu provedbe zajedničkih osnovnih standarda zaštite zrakoplovstva za sve članice Europske unije. Stoga je od 2002. godine donijela zajednička pravila za područje zaštite civilnog zrakoplovstva. Temeljni je cilj tih pravila je zaštititi ljude i robu od djela nezakonitog ometanja, [1].

Uredba br. 300/2008 Europskog parlamenta i Vijeća, koja se bavi utvrđivanjem zajedničkih pravila i temeljnih standarda o zaštiti zračnog prometa te utvrđivanjem postupaka za praćenje provedbe istih, zamijenila je inicijalnu Uredbu br. 2320/2002 Europskog parlamenta i Vijeća da bi s obzirom na nove rizike se omogućilo uvođenje novih tehnologija, [1].

Neki zajednički osnovni standardi sigurnosti uključuju:

- pregled putnika, kabine i zadržanih prtljaga
- zaštitu u zračnoj luci (kontrola pristupa, nadzor)
- zaštitne provjere i pretrage zrakoplova
- pregled tereta i pošte
- provjeru aerodromskih potreba
- zapošljavanje i obuku osoblja, [1].

U tom postupku, zadaća država članica je osigurati imenovanje jedinstvenog tijela koje je nadležno za zaštitu zračnog prometa, a koje će razviti nacionalni program zaštite civilnog zrakoplovstva te ujedno i nacionalni program kontrole kvalitete.

Operatori su dužni uspostaviti te provesti program zaštite zračne luke, kao i program zaštite zračnog prijevoznika od djela nezakonitog ometanja, [1].

Godine 2016. proveden je postupak ažuriranja čitavog niza prethodno provedbenog zakonodavstva. Naime, Komisija za provedbu Uredbe br. 2015/1998 određuje detaljne mjere kojima se provode zajednički osnovni standardi zaštite zrakoplovstva, dok se Uredba Europske komisije br. 72/2010 bavi utvrđivanjem postupaka za provođenje inspekcija Komisije u području zaštite zračnog prometa. Osim za zemlje Europske unije, ta zajednička pravila u području zaštite zračnog prometa odnose se još i na Norvešku, Island, Lihtenštajn i Švicarsku. Uredba također nudi mogućnost jednakosti zaštitnih mjera trećih zemalja čime se mogu uspostaviti zaštitni aranžmani na jednom mjestu između zemalja koje su članice Europske unije i onih koje nisu članice Europske unije (kao što je npr. postoje sa Sjedinjenim Američkim Državama, Kanadom i Crnom Gorom), [1].

2.1.1. Uredba br. 1486/2003. – provođenje inspekcije zaštite civilnog zrakoplovstva

U svrhu provođenja postupka zaštitne inspekcije civilnog zrakoplovstva usvojena je Uredba Komisije br. 1486/2003 o utvrđivanju postupaka za provođenje inspekcija Komisije u području zaštite civilnog zrakoplovstva. Njome se provjerava učinkovitost nacionalnih programa kontrole kvalitete civilnog zrakoplovstva, [2].

Države članice su dužne surađivati s Komisijom u izvršavanju njenih inspekcijskih zadataka. Osim toga, države članice su dužne poduzeti sve potrebne korake kako bi osigurale da se obavijest o inspekciji čuva u tajnosti u svrhu sprječavanja ugroženosti inspekcijskog postupka. Države članice dužne su osigurati inspektorima Komisije pristup svim sljedećim dokumentima:

- Nacionalnom programu zaštite civilnog zrakoplovstva, uključujući i nacionalni program obuke civilnog zrakoplovstva
- Nacionalni program kontrole kvalitete civilnog zrakoplovstva
- Utvrđeni program zaštite zračnih luka i zračnih prijevoznika, [2].

Države članice su dužne staviti na raspolaganje Komisiji nacionalne revizore koji mogu sudjelovati u inspekcijama kao i u pripremnim i izvještajnim fazama. Komisija mora 2 mjeseca prije obavijestiti o inspekciji odgovarajuće tijelo na čijem području će se provoditi inspekcija, [2].

Nakon provedenog izvještaja Komisija je dužna u roku od 6 tjedana nakon završetka inspekcije poslati izvještaj nadležnom tijelu. U njemu mora prikazati utvrđeno stanje i nedostatke koji su uočeni tijekom provođenja nadzora [2].

2.1.2. Uredba br. 1138/2004. – zaštitno ograničena područja u zračnim lukama

Kako bi mjere zaštite bile poduzete, prema definiciji Uredbe 1138/2004., koju je donijela Europska komisija, prostor zračne luke treba biti ograničen na:„

- nadzirano područje
- štićeno područje
- zaštitno ograničeno područje
- kritične zone zaštitno ograničenog područja“ [3].

Kod zaštitno ograničenih područja važno je ustanoviti koji je dio zračne luke prioritetno rizično područje. Ono mora obuhvaćati dijelove zračne luke kojima pristup imaju pregledani putnici, one kroz koje je moguć prolazak ili one u kojima se drži pregledana dolazeća prtljaga. Također, osoblje i posada mogu pristupiti kritičnim zonama zaštitno ograničenog područja tek nakon što prođu kroz zaštitni pregled da se utvrdi da nema zabranjenih predmeta na tom području, [3].

Kritično zaštićena područja u zračnim lukama se uspostavljaju kada više od 60 članova osoblja ima identifikacijsku karticu zračne luke koja im omogućuje pristup zaštićenom području te „kritične zone uključuju najmanje sljedeće:

- sve dijelove zračne luke u koji imaju pristup pregledani odlazeći putnici,
- sve dijelove zračne luke kroz koji može prolaziti ili u kojem se može držati pregledana odlazeća predana prtljaga, osim ako je riječ o zaštićenoj prtljazi “ [3].

Svaki dio zračne luke se smatra kritičnim dijelom zaštitno ograničenog područja sve dok:

- su na tom dijelu prisutni putnici koji odlaze, što uključuje i njihovu prtljagu
- se na tom dijelu nalazi ručna prtljaga, nakon pregleda, ako nije osigurana [3].

2.1.3. Uredba br. 820/2008. – zajednički osnovni standardi za zaštitu zrakoplovstva

Europska komisija je donijela i *Europski priručnik za civilno zrakoplovstvo* kojim se utvrđuju mjere za provedbu i tehničku prilagodbu zajedničkih osnovnih standarda koji se odnose na zaštitu zrakoplovstva kako bi isti bili ugrađeni u nacionalne programe zaštite civilnog zrakoplovstva, [4].

Pritom je određeno da države članice mogu dopustiti tehničku metodu ili postupak zaštitnih kontrola koji se koristi umjesto utvrđenih, samo pod određenim uvjetima, a to su:

- ako se koristi za potrebe ocjene novog načina provođenja navedene zaštitne kontrole
- ako to neće negativno utjecati na ukupnu razinu postignute zaštite zračnog prometa, [4].

Minimalno 4 mjeseca prije planiranog uvođenja države članice dužne su pismeno obavijestiti Europsku komisiju i ostale države članice o predloženoj novoj metodi ili postupku koji namjeravaju dopustiti, prilažući pritom procjenu koja pokazuje kako jamči da će primjena nove metode ili postupka ispuniti sve potrebne zahtjeve, [4].

U slučaju kada Europska komisija dostavi pozitivan odgovor ili, ako u roku od 3 mjeseca od primitka zahtijeva nije odgovorila, smatra se da je zahtjev usvojen. Nasuprot tome, ako je nezadovoljna predloženim, Europska komisija će u roku od 3 mjeseca po primitku obavijesti odgovoriti državi članici uz objašnjenje razloga odbijanja, [4].

2.2. Regulativa Međunarodne organizacije civilnog zrakoplovstva

Uska koordinacija država članica i sudionika temelj je europske zrakoplovne politike. Komisija je učinkoviti sudionik u svim važnim događajima Međunarodne organizacije civilnog zrakoplovstva – ICAO (eng. *International Civil Aviation Organisation*) te surađuje s glavnim partnerima trećih zemalja kao i s regionalnim organizacijama, [1].

2.2.1. Annex 17

Međunarodna organizacija civilnog zrakoplovstva – ICAO (eng. *International Civil Aviation Organisation*) specijalizirana je ustanova Ujedinjenih naroda, koja je utemeljena 1944. godine u Chicagu.

Najvažnija zakonodavna funkcija koju obavlja ICAO je formulacija i usvajanje standarda i preporučenih praksi – SARP (eng. *Standards And Recommended Practices*) za međunarodno civilno zrakoplovstvo. Oni su podijeljeni na 19 dodataka Konvencije o međunarodnom civilnom zrakoplovstvu, poznate kao Čikaška konvencija, [5].

Značaj koji je presudan za samu zaštitu zračnog prometa predstavljaju mjere koje ICAO podupire da bi se suzbila i spriječila nezakonita ometanja. Vijeće ICAO-a u ožujku 1974. usvojilo je standarde i preporučene prakse za zaštitu zračnog prometa te je donesen dokument koji se naziva Dodatak 17 (engl. *Annex 17*) Čikaške konvencije. Taj je dokument usvojen na 6 jezika i to na: engleskom, francuskom, španjolskom, ruskom, kineskom i arapskom, [5].

2.2.2. Zaštita civilnog zrakoplovstva od djela nezakonitog ometanja

Uspostava zajedničkih pravila za zaštitu civilnog zrakoplovstva od neizmjerne je važnosti kako bi se populacija unutar Europske unije zaštitila od djela nezakonitog ometanja. Također, nužno je pridržavati se i Dodatka 17., s ciljem zaštite civilnog zrakoplovstva, [6].

Bez obzira na to što u jednoj državi članici može postojati više tijela uključenih u zaštitu zrakoplovstva, svaka država članica mora imenovati jedinstveno tijelo čija je odgovornost koordinacija i nadzor nad provedbom zaštitnih standarda. Također, uz navedeno, svaka država članica dužna je napraviti nacionalni program zaštite civilnog zrakoplovstva.

S druge strane, svi zračni prijevoznici, koji primjenjuju zaštitne standarde, zaduženi su za izradu, primjenu i održavanje programa zaštite u skladu s Uredbom br. 2320/2002 te u skladu s nacionalnim programom sigurnosti civilnog zrakoplovstva koji se primjenjuje, [6].

Uredbom br. 2320/2002, Dodatka 17, utvrđuju se zajednička pravila za zaštitu civilnog zrakoplovstva od djela nezakonitih ometanja. Ta je Uredba primjenjiva za:

- sve zračne luke ili dijelove zračne luke na teritoriju države članice čije korištenje nije isključivo za vojne svrhe
- sve operatere, što uključuje i zračne prijevoznike koji pružaju usluge na zračnoj luci
- sve subjekte s primjenom zrakoplovnih zaštitnih standarda, a koji djeluju iz prostorija smještenih unutar ili izvan prostora zračne luke te pružaju razne proizvode, odnosno usluge do ili kroz zračnu luku, [6].

Prema ranije navedenom, zadatak je svake države članice sastaviti, primjenjivati i održavati nacionalni program zaštite civilnog zrakoplovstva, te su one upravo time usklađene s Uredbom. Taj program država članica propisuje odgovornosti za provedbu zajedničkih osnovnih normi te donosi opis mjera potrebnih za tu svrhu. U slučaju zahtjeva, nadležno tijelo dužno je dati na raspolaganje u pisanom obliku tražene dijelove nacionalnog programa civilnog zrakoplovstva subjektima i operatorima za koje vjeruju da imaju opravdani interes, [6].

2.3. Regulativa Republike Hrvatske

Svi propisi koji se odnose na zračni promet, a koje donose tijela Republike Hrvatske moraju biti u skladu s postojećim međunarodnim standardima. Zakon o zračnom prometu najvažniji je takav propis donesen na razini Republike Hrvatske.

2.3.1. Zakon o zračnom prometu – nadležnost i obveze provođenja mjera zaštite

Nadležnost i obaveze provođenja mjera zaštite, u prvom redu, propisani su Zakonom o zračnom prometu te se mjere zaštite zračnog prometa obavljaju u skladu s:

- odredbama Zakona o zračnom prometu
- propisom donesenim na temelju Zakona o zračnom prometu
- međunarodnim ugovorima koji obvezuju Republiku Hrvatsku, [7].

Prema navedenom, operator aerodroma za javni zračni promet „poglavito je obavezan osigurati:

1. prostor za pregled zrakoplova koji je predmetom nezakonitog ometanja
2. kontrolu i sprječavanje neovlaštenog pristupa u sigurnosno osjetljiva i štićena područja aerodroma
3. odgovarajuće prostorije za obavljanje zaštitnih pregleda putnika i stvari
4. obavljanje zaštitnih pregleda predane putničke prtljage i stvari
5. tehničku opremu za obavljanje zaštitnih pregleda predane putničke prtljage i stvari
6. obavljanje zaštitnih pregleda putnika i njihove ručne prtljage
7. tehničku opremu za obavljanje zaštitnih pregleda putnika i njihove ručne prtljage.“ [7]

Obaveza operatora aerodroma za javni zračni promet je utvrditi i primjenjivati aerodromski plan zaštite zračnoga prometa, kojeg odobrava Ministarstvo mora prometa i infrastrukture. Također, tamo gdje pristup imaju isključivo putnici, prtljaga, teret, pošta i vozila, odnosno službeno i drugo ovlašteno osoblje s valjanom identifikacijskom oznakom, operator aerodroma mora utvrditi zaštitno osjetljiva i štićena područja.

2.3.2. Nacionalno povjerenstvo za zaštitu zračnog prometa

Nacionalno povjerenstvo za zaštitu zračnog prometa osnovala je Vlada Republike Hrvatske. Svrha osnivanja Povjerenstva je poduzimanje preventivnih mjera, učinkovito djelovanje te otklanjanje posljedica uzrokovanih nezakonitim ometanjima zračnoga prometa. „Za članove Povjerenstva imenuju se predstavnici ministarstava nadležnih za poslove zračnog prometa, unutarnjih poslova, vanjskih poslova, obrane, zdravstva, financija, tijela nadležnog za nacionalnu sigurnost, Hrvatske kontrole zračne plovidbe, operatora aerodroma i operatora zrakoplova“ [7].

Nacionalno povjerenstvo za zaštitu zračnog prometa, između ostalog, zaduženo je za osnivanje lokalnog povjerenstva za zaštitu zračnog prometa na svakoj zračnoj luci za javni zračni promet. Lokalno povjerenstvo se sastoji od predstavnika subjekata koji su na bilo koji način uključeni u provedbu mjera zaštite zračnog prometa na zračnoj luci za javni zračni promet, [7].

2.3.3. Nacionalni program zaštite zračnog prometa

„Nacionalni program zaštite zračnog prometa je temeljni dokument koji sadrži sve mjere zaštite zračnog prometa od djela nezakonitog ometanja u skladu s međunarodnim ugovorima koji obvezuju Republiku Hrvatsku.“ Izdaje se na hrvatskom i engleskom jeziku, a donosi ga Vlada Republike Hrvatske, [7].

3. DJELA NEZAKONITOG OMETANJA NA ZRAČNOJ LUCI

S ciljem zaštite zračnog prometa od djela nezakonitog ometanja provodi se zaštita zračnog prometa. Nju čini skup mjera i ljudskih te materijalnih resursa. Kako bi spremno mogle odgovarati na nezakonito ometanje, zračne luke moraju održavati i provoditi postojeće mjere te ih nadopunjavati.

Djela nezakonitog ometanja su sva ona „djela ili pokušaji ugrožavanja sigurnosti civilnog zrakoplova koja podrazumijevaju, tj. uključuju, ali nisu ograničena na:

- uništenje zrakoplova u prometu
- nezakonitu otmicu zrakoplova
- uzimanje taoca u zrakoplovu u prometu ili na aerodromima
- nasilni upad u zrakoplov u prometu, zračnu luku ili službene prostorije zrakoplovnih sadržaja
- unošenje oružja, opasnih naprava ili materijala namijenjenih za počinjenje kaznenog djela u zračnu luku ili zrakoplov
- upotrebu zrakoplova u prometu s namjerom prouzrokovanja smrti, nanošenja teških tjelesnih ozljeda ili ozbiljne štete imovini ili okolišu
- prenošenje neistinitih informacija s ciljem ugrožavanja sigurnosti zrakoplova na tlu ili u letu, putnika, posade, zemaljskog osoblja i javnosti na zračnoj luci ili na prostorima sadržaja civilnog zrakoplovstva.“ [5]

3.1. Djela nezakonitog ometanja zrakoplova i zračne luke

Tehnološkim razvojem povećava se i sigurnost u zračnom prometu. Ipak, pojedinci i skupine pronalaze načine kako izvesti razne napade, odnosno djela nezakonitog ometanja zrakoplova i zračne luke. Nerijetko su usmjereni ljudskim, ali i gospodarskim žrtvama, stoga je za svaki pojedini oblik napada potrebno provesti točno određene mjere:

- **Uništenje zrakoplova u prometu**

  Europska unija donijela je pravila za područje zaštite zračnog prometa od velike važnosti za društvo i gospodarstvo kako bi se osigurao zračni prijevoz te u svrhu zaštite ljudi i organizacija od nezakonitih ometanja. Tako su, na primjer, zračnim prijevoznicima propisana pravila za prijevoz zabranjenih predmeta koji se ili ne smiju uopće prevoziti ili, ako je prijevoz dopušten, on se izvodi po točno definiranim pravilima. Pritom je svaka država ugovornica dužna provoditi zaštitnu provjeru zrakoplova prije odlaska, odnosno provesti zaštitnu pretragu zrakoplova. Zaštitna provjera zrakoplova podrazumijeva pretragu tj. inspekciju unutarnjeg dijela zrakoplova u kojem je pristup putnicima omogućen te inspekciju spremnika kako bi se otkrile sumnjive stvari, oružje, eksplozivi ili druge opasne naprave, predmeti ili tvari. Zaštitna pretraga zrakoplova podrazumijeva temeljnu inspekciju i unutrašnje i vanjske strane zrakoplova kako bi se otkrile sumnjive stvari, oružje, eksplozivi ili druge opasne naprave, predmeti ili tvari. Uz navedeno, postoji i zaštitna kontrola zrakoplova. Tim se postupkom osigurava zaštita od neovlaštenog ometanja u razdoblju od početka inspekcije do odlaska zrakoplova. U skladu s time, potrebno je da svaka država ugovornica ima formiranu zaštitnu kontrolu čiji je zadatak sprječavanje djela nezakonitog ometanja kada su zrakoplovi izvan zaštitno ograničenog područja, [8].

- **Nezakonita otmica zrakoplova:**

  Kombinacijom ljudskih i materijalnih resursa civilno se zrakoplovstvo nastoji osigurati od djela nezakonitog ometanja. Na taj su način osigurane osnove za stjecanje pristupa štićenom području i zaštitno ograničenom području. Zračne luke sastoje se od velikih površina te im je zbog toga potreban velik stupanj zaštite. Iz tog razloga je vrlo važno odrediti točne granice pojedinih područja koja su prethodno navedena u radu. One uključuju: nadzirno, štićeno, zaštitno ograničeno područje, kritične zone i demarkirane zone [3]. Zona između štićenog i nadziranog područja bi trebala biti točno vidljiva fizička barijera te bi trebala sprječavati neovlašteni pristup civilima. Kako bi pristupilo zaštitno ograničenim područjima, službeno osoblje mora imati iskaznicu za identifikaciju od zračne luke.

- **Uzimanje taoca u zrakoplovu u prometu ili na aerodromima:**

  Terorizam se definira kao primjena oružanog ili nekog drugog oblika nasilja, najčešće protiv nedužnih osoba, u svrhu ostvarivanja političkih ili nekih drugih ciljeva. Njegova osnovna obilježja su: sustavnost u upotrebi oružja, odnosno prijetnji nasiljem; uglavnom politička motivacija, tj. borba za društvene promjene, politički utjecaj ili vlast; planiran izbor izravnih žrtava, ali i onih neizravnih širenjem straha; kršenje ljudskih prava i dr. U svrhu izbjegavanja takvih situacija na zračnim lukama ili u zrakoplovima, potrebno je provesti odgovarajuće mjere zaštite, [9].

- **Nasilni upadi u zračne luke i zrakoplove**

  Osnovnu strukturu zaštite zračne luke definira prostor zračne luke koji se sastoji od zračne strane i elemenata za sigurnost zračne plovidbe. Ti elementi se ne bi trebali nalaziti na zračnoj strani, a oni mogu biti spremnici za goriva, radionavigacijskih uređaji i uređaji kontrole leta. Prolazi između zemaljske i zračne strane trebaju biti strogo kontrolirani kako neovlaštene osobe ne bi nekontrolirano prolazile. Tijekom projektiranja zračne luke, teretnih i putničkih terminala i ostalih građevina, koje imaju omogućen pristup zračnoj strani, u vidu treba imati bitne stavke kao što su Zaštitna kontrola tereta, prtljage, putnika i pošte, [5].

- **Unošenje oružja ili opasnih naprava u zračnu luku ili zrakoplov:**

  Svaka država ugovornica dužna je uspostaviti mjere kojima bi se spriječilo unošenje opasnih stvari u zrakoplov. Takve opasne stvari mogu biti eksploziv, oružje ili bilo koji drugi predmeti i tvari koje se mogu koristiti za počinjenje djela nezakonitog ometanja, [5].

- **Neovlaštena upotreba zrakoplova u prometu:**

  Neovlaštenom upotrebom zrakoplova podrazumijeva se da zrakoplovom upravlja osoba koja nema dopuštenje za korištenje zrakoplova. Svaka država ugovornica treba zahtijevati od svojih operatora da poduzimaju mjere koje bi spriječile ulazak neovlaštenih osoba tijekom leta u pilotsku kabinu, u slučaju da je to potrebno, [5].

3.2. Djela nezakonitog ometanja informacija i računalnih sustava

Osim što se u zračnom prometu djela nezakonitog ometanja usmjerena ka zrakoplovima, odnosno zračnim lukama, događaju se napadi i na informacijske te računalne sustave i mreže. Od takvih oblika nezakonitih djela također je potrebno zaštiti zračni promet provodeći propisane mjere.

3.2.1. Prenošenje dezinformacija koje narušavaju sigurnost

Kako bi naštetili infrastrukturi neke zemlje, njenom gospodarstvu ili političkim i vojnim sustavima, napadači se koriste internetom, računalnim mrežama i telekomunikacijskim sustavima kao oružjem. Sukob nalik tomu u virtualnom prostoru može biti civilnog i vojnog karaktera, no u tom slučaju internet te moderna telekomunikacijska i informacijska tehnologija predstavljaju teritorij u kojem nitko nije zaštićen od napada. Neobučeni zaposlenici, nadogradnje softvera, kvarovi opreme i postupci održavanja mogu izazvati nenamjerne prijetnje koje oštećuju podatke i nenamjerno ometaju računalne podatke. Osobe ili organizacije *cyber* napada na sustave kao primarne žrtve izabiru zaposlenike u službama zračnog prometa zbog njihove potencijalne neobučenosti. Uz potrebnu edukaciju osoblja, važno je da službe koje su zadužene za nadogradnju, tj. ažuriranje sustava u zračnom prometu adekvatno rukuju računalnim sustavima te da su na oprezu kako se prilikom ažuriranja ne bi dogodilo podmetanje *cyber* virusa, [10].

3.2.2. Kibernetičke prijetnje

Kibernetička prijetnja se definira kao pokušaj nezakonitog otkrivanja, izmjenjivanja, uništavanja, krađe, neovlaštenog pristupa ili ometanja računalne mreže i sustava. Prijetnja se ostvaruje ako se iskoristi slabost i ranjivost nekog sustava te ona može prouzročiti štetu i izazvati pogubne učinke. Zračne luke su jedna od potencijalnih meta za kibernetički napad. Međutim, sama definicija se smatra nepotpunom kada u nju nije uključen pokušaj pristupa datotekama i infiltriranja ili krađe podataka, jer se u njoj prijetnja definira samo kao mogućnost. Prijetnja se može prepoznati po nanesenoj šteti i ukradenim informacijama, [11].

Kibernetički napadi koriste zlonamjerni kod za izmjenu računalnog koda, podataka ili logike.

Kulminirajuće destruktivne posljedice mogu ugroziti podatke korisnika računala te na taj način promicati kibernetičke zločine kao što su krađa informacija i identiteta. Kibernetički napad je poznat i kao napad računalne mreže, [12].

Od kraja osamdesetih godina kibernetički napadi su se nekoliko puta razvijali kako bi iskoristili nove metode u informacijskoj tehnologiji kao sredstvo za počinjenje kibernetičkih prijetnji. Iako je važno napomenuti da se kibernetičke prijetnje još uvijek svakodnevno razvijaju, [13].

U posljednjih nekoliko godina došlo je do povećanja kibernetičkih napada, što je uočeno i u Svjetskom ekonomskom izvješću. Naime, sve veća ovisnost suvremenog društva o informacijskim i računalnim mrežama (kako u privatnom tako i u javnom sektoru) dovela je do novih kibernetičkih prijetnji, [13].

Napadači su uglavnom usmjereni na financijsku dobit ili ometanje špijunaže (uključujući korporativnu špijunažu, odnosno krađu patenata ili državnu špijunažu). Postoji niz tipova kibernetičkih prijetnji, a neki od najčešćih tipova kibernetičkih prijetnji su:

- *Backdoors*
- *Formjacking*
- *Distributed Denial of Service* - DDoS
- *Malware*
- *Cryptojacking*
- *DNS poisoning attacks* i dr. [11]

Kibernetičke prijetnje kontinuirano se razvijaju, a godišnje se javlja oko milijun novih prijetnji. Najveći dio ipak slijedi standardnu strukturu, međutim kroz razvoj one postaju sve snažnije. Ono što se javlja kao dodatan problem je nešto što stručnjaci nazivaju „napredne uporne prijetnje“ – APTs (eng. *Advanced Persistent Threats*). APTs predstavlja definiciju hakera koji upadaju u mreže te održavaju postojanost, odnosno vezu koja se ne može otkloniti ažuriranjem softvera ili ponovnim pokretanjem računala.

3.2.2.1. *Backdoors*

Backdoors, kao oblik kibernetičke prijetnje, podrazumijeva bilo koju metodu kojom ovlašteni ili neovlašteni korisnik može zaobići uobičajene sigurnosne mjere te na taj način steći pristup računalnom sustavu, mreži ili softverskoj aplikaciji, i to na visokoj razini. Nakon što se napadači uspiju priključiti, postoji mogućnost da koriste tzv. „stražnja vrata“ (*backdoor*) u svrhu krađe osobnih i financijskih podataka, a potom za instalaciju dodatnih zlonamjernih softvera.

Međutim, *backdoors* nije namijenjen samo za napadače. U nekim slučajevima ga ugrađuju i sami proizvođači softvera ili hardvera kako bi imali pristup svojoj tehnologiji. U odnosu na ostale prijetnje kod kojih se korisniku daje na znanje da postoje, *backdoors* je izuzetno diskretan. On postoji samo za određenu skupinu ljudi koji znaju na koji način dobiti vrlo jednostavan pristup određenom sustavu ili aplikaciji.

Backdoors se uglavnom klasificira kao trojanski jezik. Trojan je zlonamjerni računalni program koji se pretvara da mu cilj nije isporuka zlonamjernog softvera, krađa podataka ili otvaranje stražnjeg prostora na sustavu neke osobe. Trojanci su svestran instrument u sklopu alata za kibernetički kriminal. Dolaze u različitim oblicima, kao npr. privitak e-pošte ili preuzimanje datoteka, te isporučuju bilo koji broj prijetnji od zlonamjernog softvera.

Kako bi stvorili probleme, trojanci u pojedinim slučajevima pokazuju sposobnosti poput crva da se repliciraju i samim time šire na ostale sustave bez dodatnih naredbi kibernetičkih kriminalaca koji su ih napravili [14].

Primjer *backdoors* modela kibernetičkog napada vidljiv je u slučaju Zračne luke Bristol. Naime, prilikom tog napada isključeni su prikazi informacija o letu, prikazi podataka o prtljazi i prikazi informacija o vratima. Time su otvorene nove točke napadačima koji su pokušali dobiti nezakonit pristup informacijama. Stoga je zračna luka bila prisiljena zaustaviti brojne procese, uključujući prikaz dolaska i odlaska. Ipak, napad na jednu pristupnu točku mogao bi se koristiti za stvaranje pozadinskog pristupa drugim povezanim aplikacijama i bazama podataka. Primjerice, ako su ekrani povezani s bazom podataka zrakoplovne tvrtke koja podatke šalje drugim aplikacijama, podaci o osobnom identitetu putnika mogu biti u opasnosti. Zrakoplovne tvrtke i zračne luke sve više povezuju razne uređaje putem aplikacija dobavljača.

Jedna slaba kontrola informacijske sigurnosti u naizgled bezazlenoj aplikaciji koja se također povezuje s bazom podataka koja sadrži privatne informacije mogla bi dovesti do skupog i neugodnog kršenja prava. Uz to, *cyber* napad Zračne luke Bristol poremetio je prikupljanje i distribuciju podataka u stvarnom vremenu, prisiljavajući zaposlenike da ručno ažuriraju podatke o letu i prtljazi, a gubitak podataka doveo je do frustracije putnika, kašnjenja i propuštenih veza, što je povećalo troškove prekida poslovanja dok se zračna luka oporavljala od ovog napada, [15].

3.2.2.2. *Formjacking*

Formjacking je proces umetanja zlonamjernog *Java Script* koda u *online* obrasce plaćanja kako bi se prikupljali osjetljivi podaci korisnika. *Formjacking* je osmišljen za krađu podataka o kreditnim karticama i ostalih informacija s obrazaca za plaćanje koji se mogu zabilježiti na internetskim stranicama. Jednom kada korisnik stranice unese podatke o svojim platnim karticama na stranicu za plaćanje putem e-trgovine i klikne „Pošalji“, zlonamjeran *JavaScript* kod prikuplja unesene podatke. U okviru toga mogu se prikupljati podaci kao što su kartica za plaćanje, kućne i poslovne adrese, telefonski brojevi i niz drugih podataka. Nakon prikupljanja informacija, one se prenose na server napadača, što znači da on može te informacije koristiti za financijsku dobit ili ih može prodati, [16].

Premda ovaj model *cyber* napada nije direktno povezan sa zračnim lukama, hakeri ga koriste u napadima na zrakoplovne kompanije te uzimaju podatke osoba koje kupuju karte za let.

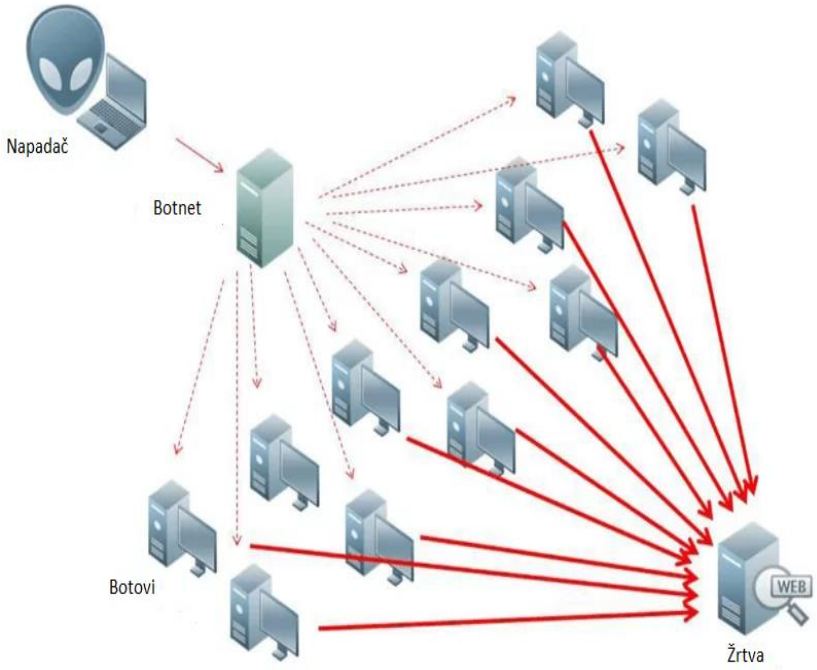
3.2.2.3. *Distributed Denial of Service – DDoS*

Distributed Denial of Service (DDoS) definira se kao isključivanje mreže ili usluge što za posljedicu ima nepristupačnost pojedinim korisnicima. Misija napada se ostvaruje prevladavajući cilj prometom ili ga preplavljuju informacijama koje pokreću pad. U obje situacije, napad DDoS-a uskraćuje legitimne korisnike kao što su zaposlenici, vlasnici računa i članovi resursa ili usluge koju očekuju, [12].

DDoS napad (slika 1.) uspostavlja kontrolu nad mrežom uređaja kako bi izveo napad. Računala i ostali uređaji se zaraze zlonamjernim softverom te se pretvaraju u robota (ili zombija). U tom slučaju napadač ima kontrolu nad mrežom zaraženih računala, koja se naziva *botnet*. Nakon uspostavljanja *botnet-a*, napadač ima mogućnost usmjeravanja uređaja slanjem ažuriranih uputa svakom *botu* na daljinu, *bot* je zaraženo računalo, [12].

Kada *botnet* odredi IP adresu žrtve, svaki *bot* će slati zahtjeve do određene mete, što potencijalno uzrokuje da ciljani poslužitelj ili mreža prepuni kapacitet, što rezultira uskraćivanjem usluge uobičajenom prometu. S obzirom da je svaki *bot* legalan internetski uređaj (osobno računalo, pametni mobitel itd.), odvajanje napadačkog prometa od uobičajenog prometa može biti relativno teško, [12].

DDoS napadi su učestalo usmjereni na internetske stranice većih organizacija kao što su trgovačke organizacije i vlade, zračne luke, medijske kompanije, trgovine i bankarstva. Iako ti napadi ne rezultiraju gubitkom ili krađom vitalnih informacija ili ostale imovine, žrtve može koštati mnogo novca i vremena za ublažavanje. DDoS se vrlo često koristi u kombinaciji da odvrati pažnju od ostalih mrežnih napada, [12].



Slika 1. Prikaz DDoS napada

Izvor: [12]

3.2.2.4. *Malware*

Malware je zlonamjerni softver koji se može odnositi na bilo koju vrstu softvera, neovisno o tome kako je strukturiran, odnosno dizajniran da uzrokuje štetu na jednom računalu, poslužitelju ili računalnoj mreži. On se može odnositi na viruse, crve, trojance, *ransomware,* špijunski softver, ali i ostale vrste štetnog softvera. Ključno razlikovanje zlonamjernog softvera je to što ono mora biti namjerno zlonamjerno. Naime, bilo koji softver koji nenamjerno nanosi štetu ne smatra se zlonamjernim softverom, [12].

Opći cilj zlonamjernog softvera je ometanje normalnog funkcioniranja uređaja. Ovaj poremećaj može biti raspoloživ u namjeri prikazivanja oglasa na uređaju bez pristanka do potpunog pristupa računalu. Stvaranje zlonamjernog softvera nastalo je kao rezultat eksperimenata i poteškoća računalnih programera, ali i otkrića komercijalnog potencijala koji je razvoj zlonamjernog softvera pretvorio u unosnu industriju crnog tržišta. U suvremenom dobu veliki broj napadača nudi pokretanje zlonamjernog softvera u zamjenu za naknadu, [12].

Najčešće vrste zlonamjernog softvera su:

- *Spyware*
- Virus
- Crvi
- Trojanski konj
- *Rootkit*
- *Ransomware*. [12]

Faktori rizika od zaraze zlonamjernim softverom su sljedeći:

- Pogreške u sigurnosti – softveri poput operativnih sustava, internetskih preglednika i dodataka preglednika mogu sadržavati ranjivosti koju napadači pritom mogu iskoristiti
- Pogreška korisnika – korisnici otvaranjem softvera s nepoznatog softvera ili podizanja računala s nepouzdanog hardvera mogu stvoriti ozbiljan rizik [12].

Dijeljenje operativnog sustava – upotreba jednog operativnog sustava za svako računalo na mreži također povećava rizik od infekcije zlonamjernog softvera; ako su svi strojevi na istom operativnom sustavu, tada postoji mogućnost da ih je jedan crv zarazio sve.

4. PRIMJERI KIBERNETIČKIH NAPADA NA ZRAČNI PROMET

Kibernetički napadi sve su češći te pogađaju svaku industriju i djelatnost. Iznimka nije ni zračni promet. Tome u prilog govore i brojni *cyber* napadi koji su izvršeni na zračne prijevoznike i zračne luke diljem svijeta. U nastavku su navedeni primjeri napada na Cathay Pacific (zračnog prijevoznika iz Hong Konga), Air Canada, Zračnu luku Hartsfield-Jackson u Atlanti, Zračnu luku Heathrow u Londonu te mrežu Vijetnamskih zračnih luka.

4.1. Kibernetički napad u Hong Kongu

Zračni prijevoznik iz Hong Konga Cathay Pacific bio je žrtva cyber napada 2018. godine. Izvršni direktor Cathay Pacifica Rupert Hogg odlučio je poboljšati zaštitne mjere nakon kibernetičkog napada. Naime, prilikom navedenog napada ugroženi su podaci čak 9,4 milijuna ljudi. Podaci su uključivali brojeve putovnica, osobnih iskaznica, povijesti putovanja, e-mail adrese te podatke o kreditnim karticama, tj. sve ono što su putnici ustupili avioprijevozniku prije leta. Iako, nasreću, podaci putnika nisu zlouporabljeni, ovaj napad pokazuje važnost mjera zaštite zračnih prijevoznika, [17].

4.2. Kibernetički napad u Kanadi

Kibernetičkim napadom na zračnog prijevoznika Air Canada ukradeni su privatni podaci korisnika s aplikacije. Kompanija je izjavila da su primijetili neobičan zahtjev koji je pokušavao ukrasti osobne podatke korisnika što ih je primoralo da se zaključa svih 1,7 milijuna računa. Unatoč zaključavanju, podatci gotovo 20.000 ljudi bili su ukradeni. Riječ je o imenima, e-mail adresama, brojevima telefona i brojevima putovnica korisnika, [17].

4.3. Kibernetički napad u Sjedinjenim Američkim državama

Na Zračnoj luci Atlanta kibernetički napad je utjecao na gašenje bežične internetske veze. Iste godine kao prijevoznik iz Hong Konga, Međunarodna zračna luka Hartsfield-Jackson pogođena je *cyber* napadom.

Točnije, informatička mreža grada Atlante napadnuta je – datoteke su bile šifrirane i ukradene, pa je Zračna luka ugasila svoj WIFI kako bi spriječila bilokakvo širenje napada na računala zračne luke, zračnih prijevoznika i računala putnika spojenih na njihovu mrežu. Premda je ovaj napad utjecao na pristup računala internetu, nije došlo do prekida letova, [17].

4.4. Kibernetički napad u Ujedinjenom Kraljevstvu

Zračna luka Heathrow bila je, za razliku od prethodnih primjera, i kažnjena zbog toga što je na nju izvršen takozvani *cyber* napad. S obzirom na to da nije uspjela zaštiti osjetljive podatke, ICO (eng. *Information Commissioner's Office*) ju je kaznio sa 120.000 funti. Naime, zaposlenik Zračne luke izgubio je USB koji je sadržavao tajne informacije, a građanin koji ga je pronašao pregledao je sve podatke i otkrio informacije o rutama putovanja engleske kraljice, imena, datume rođenja desetero ljudi te osobne podatke pedesetak zaštitara Zračne luke Heathrow koji nisu bili zaštićeni lozinkom niti šifrirani. U svom izvještaju ICO je iznio da je samo 2 %, od ukupno 6.500 radnika na Zračnoj luci Heathrow bilo educirano o zaštiti podataka. Osim kazne, Zračna luka je morala educirati svoje osoblje kako bi se u budućnosti izbjegle ovakve ili slične situacije, [17].

4.5. Kibernetički napad u Vijetnamu

Na glavne vijetnamske zračne luke izvršeni su kibernetički napadi. Sustave za objavu informaciju ugrozili su im kineski hakeri. Takvi napadi obično uzrokuju kaos u važnim prometnim čvorištima širom svijeta i potencijalno uzrokuju kašnjenja i otkazivanje letova, pa čak i povećane zaštitne uzbune, s obzirom na to koliko se napada događa u svijetu, a povezuje se sa terorizmom.

Na vijetnamskim međunarodnim zračnim lukama Noi Bai u Hanoiu i Tan Son Nhat u Ho Chi Minh napadi su se manifestirali na ekranima koji sadržavaju informacije o letovima. Naime, pojavile su se uvredljive poruke na engleskom jeziku protiv Vijetnama i Filipina. Proboji i kvarovi također su primijećeni i u drugim zračnim lukama.

Mnogi prijevoznici koji posluju na zahvaćenim zračnim lukama bili su primorani isključiti šaltere za *check-in* i prebaciti se na ručne metode kako bi se raspored letenja održao bez kašnjenja.

Uz navedeno, osobni podaci otprilike 411.000 putnika bili su izloženi zbog napada na internetske stranica vijetnamski zračnih prijevoznika.

Prema slikama s ekrana za informacije o letu, otkriveno je da su hakeri odgovorni za ovaj kibernetički napad je kineska „1937CN“ grupa. Oni su, između ostalog, preuzeli odgovornost za još više od 1.000 napada na vijetnamske internetske stranice.

Iako je ovaj kibernetički napad prouzrokovao neregularnost na vijetnamskim zračnim lukama, odgovarajuće institucije uspjele su blokirati napadače od uzrokovanja veće štete, [18].

5. PREVENTIVNE ZAŠTITNE MJERE I METODE

Za zaštitu zračnih luka potrebno unaprijediti sustave s obzirom na razvijajuću tehnologiju kibernetičkih napada što uključuje pravilno upravljanje sustavima svih sudionika.

5.1. Zaštitne mjere za zračne luke

Zaštitne mjere zračnih luka podijeljene su u tri glavne kategorije:

- tehničke
- organizacijske
- standarde, [19].

Od tri navedene kategorije u zračnim lukama za suzbijanje kibernetičkih napada najvažniju ulogu imaju tehničke mjere zaštite koje svaka zračna luka mora provoditi kako bi se obranila od mogućih napada.

Postoji mnogo učinkovitih tehničkih mjera za borbu protiv kibernetičkih napada, a neke od njih su, [19]:

- ***Antimalware*:** Sva računala trebala bi koristiti *anti-malware* softver kako bi mogli otkriti, ukloniti ili blokirati zlobne softvere. Oni mogu omogućiti zaštitu protiv instalacije zlonamjernih softvera na računalo, takav tip zaštite radi na isti način kao i *antivirus* zaštita.
- **Ažuriranja softvera i hardvera:** Svaki softver ili hardver trebao bi se često ažurirati jer se u tim ažuriranjima nalaze nadogradnje za sustave zaštite koji su izloženi kibernetičkim napadima.
- **Vatrozid:** Granica mrežne infrastrukture zračne luke trebala bi biti zaštićena mnogobrojnim vatrozidima kako bi se blokirale nepouzdane konekcije između mreža. Za poboljšanje sigurnosti mreže potrebno je poduzeti puno bolji obrambeni pristup.
- **Sustav za otkrivanje prodora:** Odnosi se na nadzor softverskih i hardverskih uređaja putem mreže.

Može se kategorizirati kao mrežni koji je usredotočen na analizu mrežnog prometa i koji je sposoban analizirati aktivnosti i obavještavati u slučaju događaja poput neovlaštenog pristupa sustavu, zaobilaženju identifikacija i promjena sustavnih datoteka. Ne koristi se kod manje značajnih zračnih luka.

- **Provjera autentičnosti korisnika:** Trebala bi zaštiti informacijsko-komunikacijske uređaje, dok je za osjetljive ili udaljene usluge potrebna višestrana provjera autentičnosti.
- **Promjena zadanih postavki uređaja:** Uređaji koji su spojeni na mrežu zračne luke trebaju biti posebno programirani kako bi se promijenile zadane tvorničke lozinke. Također, kada se uređaji ne koriste, potrebno je onemogućiti daljinsku kontrolu uređaja kako bi spriječili kibernetički napadi.
- **Šifriranje podataka:** Koristi se za zaštitu osjetljivih informacija koje se razmjenjuju putem mreže, a moguće ih je jednostavno presresti i prikupiti podatke.
- **Kontrola osobnih uređaja:** Zračne luke trebale bi spriječiti svoje zaposlenike u povezivanju vlastitih osobnih uređaja na mrežne sustave zračne luke. U suprotnom bi trebalo primijeniti puno učinkovitije metode tehničkih kontrola kako bi se zaštitila zračna luka i njena mrežna infrastruktura od ugroženih uređaja.
- **Planovi oporavka informacijsko-komunikacijske mreže:** U slučaju nužde, treba uspostaviti tehničke procedure za vraćanje u rad informacijsko-komunikacijske mreže. Tehnički i organizacijski odjeli moraju biti uključeni u planove za oporavak mreže. Ljudi koji su uključeni u oporavak moraju imati jasno definirane uloge i redoslijed radnji koje trebaju izvesti.
- **Primjena zaštitnog plana:** Siguran plan trebao bi biti dio sustava, usluga i tehnologije. Preporučljivo je kombinirati ga sa sigurnosnim zahtjevima i zaštitom od rizika zračne luke, [19].

5.2. Preventivne zaštitne mjere prema ICAO

Svaka država članica ugovornica dužna je uspostaviti mjere kako bi spriječila unos opasnih stvari, oružja, eksploziva ili nekih drugih opasnih tvari, naprava ili predmeta koji se koriste za počinjenje djela nezakonitog ometanja u prijevozu ili neovlašteno unošenje u zrakoplov civilnog zrakoplovstva. Sredstva za uspostavu navedenih mjera su u nadležnosti država članica.

ICAO propisuje zaštitne mjere za kontrolu pristupa, putnike, prtljagu, zrakoplove, teret, poštu i svu drugu robu, posebnu kategoriju putnika, zemaljsku stranu aerodroma, ali i mjere za *cyber* prijetnje. Također, ICAO donosi i preporuku uvođenja nepredvidivih zaštitnih mjera. Pomoću njih povećava se učinak zastrašivanja usmjeren ka potencijalnim počiniteljima djela nezakonitog ometanja, [5].

5.2.1. Mjere vezane za kibernetičke prijetnje

Kako bi se zaštitili povjerljivost, integritet i raspoloživost kritičnih sustava informacijskih i komunikacijskih tehnologija te povjerljivost podataka koji se koriste u civilnom zrakoplovstvu od ometanja koje može ugroziti sigurnost civilnog zrakoplovstva, preporuča se da svaka država ugovornica osigura odgovarajuće mjere u skladu s procjenom rizika izvedenom od strane odgovornih vlasti. Također, svaka država ugovornica treba poticati subjekte, koji su uključeni ili dogovorni za primjenu različitih aspekata Nacionalnog programa zaštite civilnog zrakoplovstva, da identificiraju svoje sustave informiranja, komunikacijskih tehnologija i podataka uključujući prijetnje i ranjivost, [5]. Razlog tome je taj što se razvojem tehnologija, gradnjom suvremenijih zračnih luka te sve većom upotrebom informacijskih i komunikacijskih tehnoloških sustava, povećava opasnost od kibernetičkih napada.

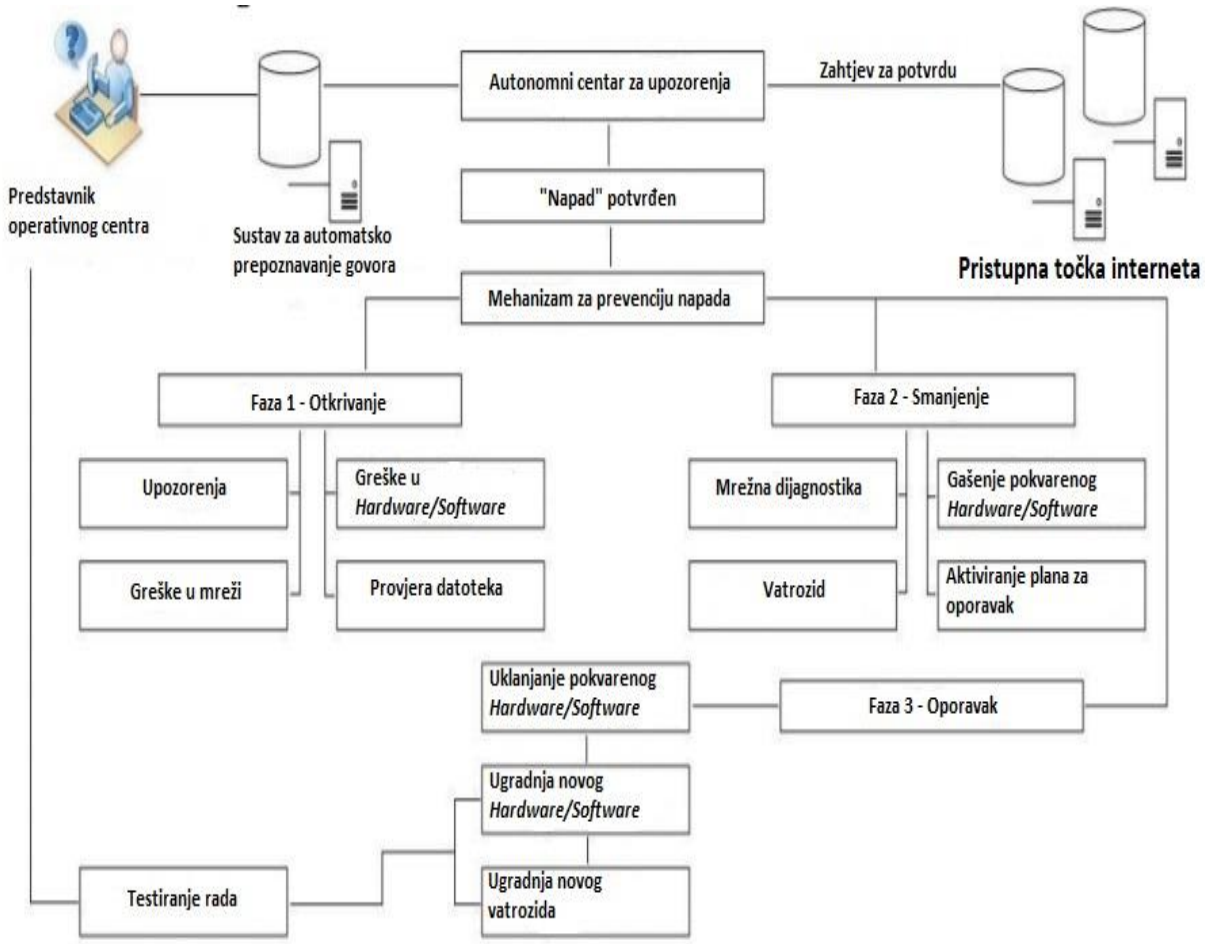
Spomenuto je ranije da postoji niz tipova kibernetičkih prijetnji te su neke od njih i nabrojane. One koje se vrlo često pojavljuju su *Malware* i DDoS, a mjere prevencije koje se kod ovih tipova kibernetičkih prijetnji primjenjuju su sljedeće:

- Mjere prevencije *Malware* napada na zračnu luku – Prije svega treba napomenuti da je *Malware* softver koji žrtvu napad kombinacijom napada i može biti skriven u bilo kojem programu koji se svakodnevno koristi, [20].

Kako bi se to izbjeglo, preporučena je edukacija zaštitnog osoblja zračne luke o mogućnostima prikrivanja masivnog kibernetičkog napada s lažnim kibernetičkim napadom.

Također, da bi se smanjio rizik pojavljivanja takvih situacija, određene komponente hardvera ili softvera mogu biti umetnute u infrastrukturnu mrežu da se neprekidno prate kretanja opreme zračne luke. Drugi način za sprječavanje takvih *Malware* napada je da se analiziraju slični napadi i razviju bolji i efikasniji zaštitni algoritmi za samostalno praćenje zračnog prometa koji će brzo reagirati ako se posumnja u velik broj kašnjenja zrakoplova, [20].

- Mjere prevencije DDos napada na zračnu luku dijele se na sljedeće:
  a) sveobuhvatna zaštita – metoda korištena od strane ISPs (eng. *Internet service providers*) u svrhu prevencije i identifikacije potencijalnih DDoS napada. Internetski poslužitelji su u mogućnosti filtrirati sve zahtjeve dobivene od stranih nesigurnih izvora. Na taj način ISPs može smanjiti preveliki internetski promet i odobriti pouzdane zahtjeve koji žele pristupiti IP adresi zračne luke. Neke IP adrese mogu se blokirati ako je potrebno.
  b) alternativni način – koristi se u prevenciji kibernetičkih napada pomoću razvoja sporedne internetske mreže i dodjele različitih IP adresa koje će se koristiti samo u hitnim situacijama.
  c) *blackholing* – kako bi unaprijedili efikasnost zaštitnog mehanizma, potrebno je uvesti uređaje velikih brzina koji su osmišljeni isključivo za mrežna sučelja. Uloga tih uređaja je kontinuirano praćenje aktivnosti i postojećeg prometa određenih IP adresa zračne luke. U slučaju otkrivanja napada, promet će biti preusmjeren na uređaj za blokiranje. Poslužitelj će biti automatski obaviješten o napadima na određene IP adrese te će automatski blokirati sav internetski promet prema njima. Procedura koja je vrlo važna u ovoj fazi je minimiziranje ljudskog faktora u nadziranju internetskog prometa. Prilikom poziva o kibernetičkom napadu, automatski prepoznavatelj govora aktivirat će mehanizme za zaštitu, [20].



Slika 2. Sustav za prepoznavanje govora

Izvor: [20]

5.2.2. Ostale mjere

Uz postojeće mjere za kibernetičke prijetnje, potrebno je provoditi niz drugih mjera u svrhu zaštite zračnog prometa, a koje su propisane od strane ICAO te se odnose na sljedeće:

- **Mjere vezane za kontrolu pristupa**

  Zaštitno ograničena područja moraju biti uspostavljena na svakoj zračnoj luci. Granica između ograničenih područja i ostalih područja treba biti jasno definirana. Uvođenjem granica u ograničenim područjima smanjuje se neovlašteno kretanje osoblja unutar zračne luke, a istovremeno održava se praktičan sustav za kontrolu pristupa. Osobe koje nisu ovlaštene ili kojima nije odobren pristup u područja treba ispitati te, ako ne mogu dokazati neovlaštenu prisutnost, prijaviti nadležnim službama zračne luke. Osobe koje nisu prošle zaposlenici moraju imati stalnu pratnju unutar zaštitno ograničenih područja. S druge strane, osobe kojima su izdane dozvole za zračnu luku ili imaju identifikacijsku iskaznicu zračne luke trebaju biti podvrgnute povremenim ponovnim provjerama od strane nadležnih službа. Izdavanje identifikacijskih iskaznica za ograničeno područje izdaje se samo onima kojima je potrebna za ulazak u ograničena područja. Identifikacijske iskaznice imaju određeno vrijeme valjanosti, a korisnici ih trebaju moraju na vidljivome mjestu cijelo vrijeme unutar ograničenih područja, [21].
- **Mjere vezane za zrakoplov**

  Uključuju provedbu kontrole pristupa zrakoplovima, provođenja zaštitnih pregleda zrakoplova, kao i pregled zrakoplova kako putnici ne bi ostavili stvari unutar zrakoplova, [21].
- **Mjere vezane za putnike i njihovu kabinsku prtljagu**

  Putnike koji su sumnjivi zbog svojeg ponašanja ili nakon ispitivanja, potrebno je podvrgnuti detaljnijoj provjeri zajedno s njihovom prtljagom. Tamo gdje je to izvedivo, putnici koji su pregledani trebaju biti fizički odvojeni zidovima ili pregradama, a tamo gdje to nije izvedivo potrebno je koristiti ručne kontrole pomoću osoblja.

  Kod zračnih luka koje nisu dizajnirane tako da je moguća fizička odvojenost između dolaznih i odlaznih putnika, prostor za sjedenje u čekaonicama treba dizajnirati tako da se smanji mogućnost ostavljanja predmeta od strane dolazećih putnika za putnike koji odlaze.

Treba razviti proces procjene rizika za svakog putnika kako bi se olakšalo njihovo kretanje po zračnoj luci. Zračne luke moraju osigurati prikaz jasnih uputstva i informacija putnicima prije zaštitne kontrolne točke kako bi ih pripremili na sigurnosni pregled i uputili u pogledu ograničenja za tekućine i gelove u ručnoj prtljazi, [21].

- **Mjere vezane za predanu prtljagu**

  Sustavi za rukovanje prtljagom trebaju biti zaštićeni i pristup njima mora biti omogućen samo ovlaštenom osoblju, tako se mogu spriječiti pljačke, neovlašteno rukovanje prtljagom te postavljanje zabranjenih predmeta u prtljagu od neovlaštenih osoba. Takva područja trebaju biti dio zaštitno ograničenog područja. Također, potrebno je uspostaviti procedure za procjenu rizika pri postupku s neidentificiranom prtljagom [21].

- **Mjere vezane za teret, poštu i ostale stvari**

  Kako bi se osigurao siguran prijevoz tereta i pošte širom svijeta, države trebaju kombinirati zaštitne sustave za pregled tereta i pošte kako bi razvile usklađene mjere osiguranja.

  Te mjere moraju se primjenjivati jednako na sve opskrbljivače kako bi se smanjio rizik od ukrcaja stvari namijenjenih za nezakonito ometanje u zrakoplov. Provjeru treba provoditi na kontrolnim točkama prije i unutar ograničenih područja. To može biti postignuto nasumičnim pregledima ili sigurnom dostavom tereta ako je taj predmet bio zaštićen od neovlaštenog utjecaja. Prijevoz robe mora imati odgovarajući nadzor. Nasumične pretrage robe trebaju biti provedene kod bilo koje osobe uključujući i posadu. Prije leta potrebno je obaviti preglede kako se ne bi oružje ili neke druge opasne stvari postavile u zrakoplov. Posebnu pozornost daje se zrakoplovima koji su stajali duži period, noćili na zračnoj luci ili bili na tehničkoj provjeri, a koji moraju biti zaštićeni od prilaza neovlaštenih osoba [21].

- **Mjere vezane za posebne kategorije putnika**

  Potencijalno opasnim putnicima smatraju se, osim onih koji su uključeni u sudske ili pravne procese te osim osoba koje u sklopu dužnosti nose oružje [5], i svi oni koji narušavaju red u zrakoplovu.

  Problem nepristojnih putnika je ozbiljan, ali najveći rizik je u letu kada takvi putnici mogu narušiti sigurnost leta i ostalih putnika. Postoji rizik i za putnike u terminalu od nepristojnih putnika, a najčešći razlog takvog ponašanja je alkohol.

  Zračne luke moraju osigurati procedure za takve i slične događaje (koji obično zahtijevaju intervenciju policije) te odgovarajuće osposobljeno osoblje.

Nepristojni putnici najčešće pokazuju nepristojno ponašanje već prilikom ukrcaja u zrakoplov. Djelatnici zračne luke dužni su obavijestiti zračnog prijevoznika i policiju kada uoče putnika koji se nepristojno ponaša. Zračni prijevoznik određuje je li taj putnik sposoban za ukrcaj na zrakoplov. Osobe koje su pod sudskim nalogom na letu (npr. deportirci ili zatvorenici itd.) predstavljaju veći rizik od normalnih putnika. Potrebno je da vlade država surađuju sa zračnim lukama i zračnim prijevoznicima kako bi se takvi postupci prijevoza sveli na minimalne rizike uz stalnu pratnju [21].

- **Mjere vezane za zemaljsku stranu**

Prilikom planiranja zračne luke treba pažljivo razmotriti sve postojeće i predvidljive elemente zaštite. Država, zračna luka i stručnjaci za zaštitu zračnih luka trebaju zajedno surađivati kako bi postigli najbolje rezultate. Dizajn novih objekata trebao bi uzeti u obzir: planove za nepredviđene slučajeve kako bi se smanjio rizik od smrtonosnih napada, odvajanje onih koji su prošli zaštitnu kontrolu od onih koji nisu, pregled putnika i njihove ručne prtljage, pružanje posebnih mjera za rizične putnike, pregled prijavljene i transferne prtljage. Zračne luke moraju razmotriti dizajn infrastrukture kako bi ublažile prijetnju od napada, pogotovo prilikom nadogradnje ili izgradnje novih objekata. Taj dizajn treba uključivati: zaštitu od eksplozije, neprobojna stakla, betonske stupiće i druge prepreke za sprječavanje prodora automobila, područja za iskrcaj i ukrcaj putnika ispred terminala koja su odvojena pješačkim stazama, planiranje prostora radi smanjenja okupljanja ljudi. Također, potrebno je da zračne luke smanje pristupna područja (poput terasa) gdje bi potencijalni napadač ili bombaš mogao imat pristup prepunim javnim površinama te smanjiti mjesta gdje se mogu sakriti predmeti (kao što su neprozirne kante za smeće). Prilikom planiranja izgradnje novih zgrada ili kuća u okolici zračne luke treba se pripaziti na smjer pogleda terasa, balkona ili prozora s pogledom na zračnu luku, a koji mogu ugroziti sigurnost iste. Zračne luke trebaju inzistirati na komunikaciji osoblja i putnika kao sredstvo prepoznavanja sumnjivog ponašanja.

To može dovesti do toga da putnici sami prijavljuju sumnjivo ponašanje i ostavljenu prtljagu. Zračne luke trebaju osigurati obuku o sigurnosti za cjelokupno osoblje (zaposlenike zračne luke, građane i one koji nisu direktno uključeni u zaštitu) kako bi prepoznali na vrijeme sumnjivo ponašanje i prijavili ga, [21].

6. ZAKLJUČAK

Iako se zračni promet smatra jednom od najsigurnijih vrsta prometa, često je meta raznovrsnih djela nezakonitog ometanja. Svaka država članica Europske unije, pa tako i Republika Hrvatska, provodi zaštitne mjere u skladu s vlastitim propisima, regulativom Europske komisije i ICAO sprječavajući na taj način brojna djela nezakonitog ometanja. Time se, ujedno, podiže i razina zaštite te pojačava sigurnost u zračnom prometu.

Mjere zaštite zračnog prometa, između ostalog, poboljšavaju se i standardiziraju zahvaljujući tehnološkom razvoju. Tehnološki razvoj, također, omogućuje i osobama čija je namjera ugrožavanje sigurnosti da koriste nove načine i oblike djela nezakonitog ometanja. U prvom redu se to odnosi na *cyber* kriminalce. Informacijski i komunikacijski sustavi rapidnom brzinom razvijaju, a s njima i zlonamjerni softveri i ostali programi.

Kibernetičke prijetnje danas su najučestaliji oblik djela nezakonitog ometanja u zračnom prometu. Podrazumijevaju svako nezakonito otkrivanje, izmjenjivanje, uništavanje, krađu, neovlašteni pristup ili ometanje računalne mreže i sustava, a cilj im je izazvati štetu ili neke druge pogubne učinke. Upravo se i prepoznaju po nanesenoj šteti i ukradenim informacijama. Stoga postojanje sigurnosnih programa i zaštitnih mjera u zračnom prometu nije jedino rješenje za ovaj, ali i svaki drugi oblik djela nezakonitog ometanja. Potrebno je neprestano raditi na ažuriranju sigurnosnih programa, izmjenjivati i nadopunjavati postojeće mjere zaštite, ali i educirati osoblje zaduženo za zaštitu. Također, važno je i poraditi na učestalijem i učinkovitijem otkrivanju potencijalnih prijetnji. Prvi korak ka tome je ulaganje u samu zaštitnu infrastrukturu.

Dakle, samo s adekvatnim mjerama zaštite, suvremenom tehnologijom i infrastrukturom te kvalitetno osposobljenim osobljem može se ostvariti visoka razina zaštite u zračnom prometu i uspješno odgovoriti na nove oblike napada i prijetnji u budućnosti.

LITERATURA

[1] An official EU website. Mobility and Transport. Preuzeto sa: https://ec.europa.eu/transport/modes/air/security_en [Pristupljeno: srpanj 2020.].

[2] Commission regulation (EC) No 1406/2003. Procedures for conducting inspections in the civil aviation security. Official Journal of the Europen Union. Preuzeto sa: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003R1486&f rom=EN [Pristupljeno: srpanj 2020.].

[3] Commission regulation (EC) No 1138/2004. Security restricted areas at airports. Official Journal of the Europen Union. Preuzeto sa: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:02015R1998-20200702 [Pristupljeno: rujan 2020.].

[4] Commission regulation (EC) No 820/2008. Common basic standard on aviation security. Official Journal of the European Union. Preuzeto sa: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008R0820&from=EN [Pristupljeno: srpanj 2020.].

[5] International Civil Organization. Annex 17 to the Convention on International Civil Aviation: Security, Safeguarding International Civil Aviation Against Acts of Unlawful Interference. Ninth Edition. Montreal: 2011. Preuzeto sa: https://www.pilot18.com/icao-annex-17-security/ [Pristupljeno: kolovoz 2020.].

[6] Commission regulation (EC) No 2320/2002. Civil aviation security. Official Journal of the Europen Union. Preuzeto sa: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008R0300 [Pristupljeno: kolovoz 2020.].

[7] Zakon o zračnom prometu (NN 69/2009). Preuzeto sa: http://www.propisi.hr/print.php?id=9330 [Pristupljeno, rujan 2020.].

[8] Hellenberg T. Vissuri P. Nicander L. Securing Air Traffic (Case CBRN Terrorism). Helsinki: Aleksanteri Institute of University of Helsinki. 2011.

[9] Wisnewski J. J. Torture, Terrorism, and the Use of Violence Cambridge: Cambridge Scholars Publishing. 2008.

[10] Civil Air Navigation Services Organisation. Cyber Security and Risk Assessment Guide Hoofddorp. CANSO. 2017.

[11] PhonenixNAP GLOBAL IT SERVICES. Preuzeto sa: https://phoenixnap.com/blog/cyber-security-attack-types [Pristupljeno: kolovoz 2020.].

[12] Blog netwrix. Preuzeto sa: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ [Pristupljeno: rujan 2020.].

[13] World Econnomic Forum. The Global Risks Report 2019. 13th Edition, Geneva: 2019. Preuzeto sa: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf [Pristupljeno: kolovoz 2020.].

[14] Bank info security. Preuzeto sa: https://www.bankinfosecurity.com/intrusions-take-months-to-detect-a-7158 [Pristupljeno: rujan 2020.].

[15] Acronis. Preuzeto sa: https://www.acronis.com/en-us/blog/posts/ransomware-attack-against-bristol-airport-shows-need-smart-secure-digital-infrastructure [Pristupljeno: rujan 2020.].

[16] Norton: Emerging Threats. Preuzeto sa: https://us.norton.com/internetsecurity-emerging-threats-what-is-formjacking.html [Pristupljeno: rujan 2020.]

[17] Airport Technology. Preuzeto sa: https://www.airport-technology.com/features/five-times-airports-were-involved-in-cyberattacks-and-data-breaches/ [Pristupljeno: kolovoz 2020.].

[18] ZDNet. Preuzeto sa: https://www.zdnet.com/article/chinese-hackers-take-down-vietnam-airport-systems/ [Pristupljeno: rujan 2020.].

[19] Lykou G. Anagnostopoulou A. Gritzalis D. Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience. Atena: Athens University of Economics & Business. 2018. Preuzeto sa: https://www.researchgate.net/publication/328985624_Implementing_Cyber-Security_Measures_in_Airports_to_Improve_Cyber-Resilience#read [Pristupljeno: kolovoz 2020.].

[20] Suciu G. Scheianu1 A. Vulpe A. Petre1 I. Suciu V. Cyber-attacks – the Impact over Airports Security and Prevention Modalities. Bukurešt: BEIA Consult International. Preuzeto sa: http://www.beiaro.eu/wp-content/uploads/2018/12/Cyber-attacks-%E2%80%93-the-Impact-over-Airports-Security-and-Prevention-Modalities.pdf [Pristupljeno: kolovoz 2020.].

[21] Airports Council International. Policy and Recommended Practices Handbook. Eight edition. Montreal: 2016.

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Zaštita zračnih luka od kibernetičkih prijetnji**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 09/09/2020

Dino Jakšić

(potpis)

POPIS SLIKA