Cyber prijetnje u zračnom prometu

Nikolić, Tomislav

Undergraduate thesis / Završni rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:845811

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Tomislav Nikolić

CYBER PRIJETNJE U ZRAČNOM PROMETU

ZAVRŠNI RAD

Zagreb, 2017.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 24. travnja 2017.

Zavod: **Zavod za zračni promet**
Predmet: **Zaštita u zračnom prometu**

ZAVRŠNI ZADATAK br. 3965

Pristupnik: **Tomislav Nikolić (0135233766)**
Studij: Promet
Smjer: Zračni promet

Zadatak: **Cyber prijetnje u zračnom prometu**

Opis zadatka:

U uvodnim postavkama potrebno je opisati predmet istraživanja, objasniti svrhu i cilj istraživanja te dati kratak pregled strukture završnog rada. Prikazati motive cyber prijetnji i napada u zračnom prometu te njihov utjecaj na podsustave zračnog prometa (zračne luke, prijevozništvo i kontrolu zračne plovidbe). Objasniti metodologiju procjene zaštitnog rizika i identificirati metode zaštite. Interpretirati međunarodne standarde i preporuke za zaštitu civilnog zrakoplovstva od cyber napada. Izvesti zaključke i argumentirati dobivene rezultate.

Zadatak uručen pristupniku: 28. travnja 2017.

Mentor:

Arijana Modić

Arijana Modić, mag. ing. traff.

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

CYBER PRIJETNJE U ZRAČNOM PROMETU

CYBER THREATS IN AIR TRAFFIC

Mentor: Arijana Modić, mag.ing.traff.

Student: Tomislav Nikolić
JMBAG: 0135233766

Zagreb, rujan 2017.

SAŽETAK

Jako brzi razvoj tehnologije i tehnoloških sustava danas predstavlja sve veću opasnost od *cyber* napada, osobito u zračnom prometu. Protok informacija kroz različite tehnološke sustave predstavlja bolju učinkovitost i produktivnost, no samim time i veliku opasnost od *cyber* napada. Budući da se informacije u zračnom prometu sve manje dijele putem *point-to-point* komunikacije, opasnost od *cyber* napada je sve izglednija. Određene službe zračnog prometa imaju zadatak razviti planove i strategije koje će osigurati što veću sigurnost u zračnom prometu a istovremeno i manje rizike suočavanja sa *cyber* prijetnjama. Njihov način djelovanja prvenstveno se odnosi na metode i preporuke koje donose u poboljšanju borbe protiv *cyber* prijetnji te koje osiguravaju bolju sigurnost zrakoplova, zaposlenika u zračnim službama i civila. *Cyber* prijetnje mogu utjecati na svaki dio zračnog kompleksa pri čemu određene službe zračnog prometa imaju zadatak identificirati, analizirati i odrediti metodu suočavanja sa *cyber* prijetnjama.

KLJUČNE RIJEČI: *cyber* prijetnje; procjena *cyber* rizika; zaštita od *cyber* napada

SUMMARY

The very rapid development of technology and technological systems today poses an ever greater risk of cyber attacks especially in air traffic. The flow of information through different technology systems is more efficient and productive, but is also a major threat to cyber attacks. Since air traffic information is less shared through point-to-point communication, the danger of cyber attacks is becoming more and more likely. Certain air traffic services have a task to develop a strategies and plans that will ensure greater safety in air traffic while at the same time less risk of facing cyber threats. Their mode of action is primarily related to the methods and recommendations they bring to improve the fight against cyber threats and to ensure better safety of aircraft, airline staff and civilians. Cyber threats can affect every part of the air complex where certain air traffic services have the task of identifying, analyzing and determining the method of coping with cyber threats.

KEY WORDS: cyber threats; cyber risk assessment; protection from cyber attacks

Sadržaj

1. UVOD 1

2. MOTIVI *CYBER* PRIJETNJI 3

2.1. Izvori i podjela cyber prijetnji 3

2.2. Razine cyber prijetnji prema stupnju sigurnosti 4

3. UTJECAJ *CYBER* NAPADA NA PODSUSTAVE ZRAČNOG PROMETA 7

3.1. Utjecaj *cyber* napada na zračne luke 7

3.2. Utjecaj *cyber* napada na prijevoznike u zračnom prometu 8

3.3. Utjecaj *cyber* napada na kontrolu zračne plovidbe 9

4. METODOLOGIJA PROCJENE *CYBER* RIZIKA U PODSUSTAVIMA ZRAČNOG PROMETA 10

4.1. Identifikacija, analiza i procjena *cyber* rizika 11

4.2. Razine posljedica javljanja *cyber* rizika 13

4.3. Procjena vjerojatnosti nastanka *cyber* rizika 13

5. PROVOĐENJE PREVENTIVNIH MJERA I METODE ZAŠTITE 15

5.1. Područja provođenja preventivnih mjera 15

5.2. Zaštita u službi upravljanja zračnim prometom 16

5.3. Razvoj *Cybersecurity* programa 16

5.4. Načelo zaštite od *cyber* napada 18

6. MEĐUNARODNI STANDARDI I PREPORUKE ZA ZAŠTITU CIVILNOG ZRAKOPLOVSTVA OD *CYBER* NAPADA 20

6.1. Organizacije uključene u program zaštite civilnog zrakoplovstva od *cyber* napada 20

6.2. Međunarodni standardi i preporuke 21

7. ZAKLJUČAK 24

POPIS KRATICA 26

POPIS LITERATURE 27

POPIS TABLICA 28

POPIS SLIKA 29

1. UVOD

Cyber prijetnje u 21. stoljeću za zračni promet predstavljaju veliku opasnost. Budući da se napretkom tehnologije i razvojem novih sustava zračni promet sve više okreće automatizaciji, opasnost od *cyber* napada svakim danom postaje sve veća. Najveći problem u suočavanju sa *cyber* prijetnjama predstavlja razvoj tehnologije jer *hackeri* ili potencijalni teroristi koriste sofisticiranije sustave pa ih je samim time teže locirati. Ipak pravovremenim sigurnosnim mjerama, razvojem strategija i planova moguće je brzo i učinkovito odgovoriti na *cyber* prijetnje.

Motivi *cyber* prijetnji su različiti i svaki od njih predstavlja određenu razinu opasnosti i utjecaj na podsustave zračnog prometa. Kako bi se pravovremeno uklonile *cyber* prijetnje određuje se metodologija procjene rizika uz provođenje mjera sigurnosti i zaštite. Da bi zračni promet u globalnom smislu bio sigurniji, uvedeni su određeni međunarodni standardi i preporuke u cilju zaštite od *cyber* prijetnji. Cilj završnog rada je predstaviti *cyber* prijetnje kao ozbiljan problem u zračnom prometu te temeljem procjene rizika uz standarde i preporuke pružiti što bolju zaštitu i sigurnost od *cyber* prijetnji u civilnom zrakoplovstvu. Naslov završnog rada je: ***Cyber* prijetnje u zračnom prometu**. Rad je podijeljen u sedam cjelina:

1. Uvod
2. Motivi *cyber* prijetnji
3. Utjecaj *cyber* napada na podsustave zračnog prometa
4. Metodologija procjene *cyber* rizika u podsustavima zračnog prometa
5. Provođenje preventivnih mjera i metode zaštite
6. Međunarodni standardi i preporuke za zaštitu civilnog zrakoplovstva od *cyber* napada
7. Zaključak.

U drugom poglavlju su opisani različiti motivi *cyber* prijetnji, potencijalni izvori *cyber* prijetnji koji zbog mnogih stvari mogu predstavljati opasnost zračnom prometu te razine *cyber* prijetnji prema stupnju sigurnosti koje se određuju identifikacijom i analizom *cyber* prijetnje.

U trećem poglavlju prikazani su utjecaji *cyber* napada na podsustave zračnog prometa. Prikazani su utjecaji *cyber* napada na sustave zračne luke pri čemu dolazi do izražaja sama funkcionalnost zračne luke, na prijevoznike u zračnom prometu pri čemu redovitost i sigurnost u odvijanju zračnog prometa imaju najveću ulogu te na sustave kontrole zračne plovidbe gdje najveći problem od *cyber* napada postaje sigurnost zrakoplova.

Četvrto poglavlje obuhvaća metodologiju procjene *cyber* rizika u podsustavima zračnog prometa. Opisani su koraci identifikacije, analize i procjene *cyber* rizika koji imaju direktan pristup u rješavanju *cyber* prijetnji. Navedene su razine posljedica javljanja *cyber* rizika koje prema svom opsegu utječu funkcionalnost dijelova zračnog prometa. Radi dugoročnog planiranja zaštite od *cyber* napada, opisana je i učestalost potrebe za analizom *cyber* rizika u podsustavima zračnog prometa.

U petom poglavlju prikazano je provođenje preventivnih mjera i metoda zaštite od *cyber* rizika. Navedena su područja zračnog prometa gdje se provode preventivne mjere i metode zaštite. Prikazan je razvoj *Cybersecurity* programa koji predstavlja prvi obrambeni mehnizam u suočavanju sa *cyber* napadima te načelo zaštite od *cyber* napada koje ima jasan i direktan pristup u rješavanju potencijalne prijetnje.

Šesto poglavlje obuhvaća međunarodne standarde i preporuke za zaštitu civilnog zrakoplovstva od *cyber* napada. Navedene su organizacije koje sudjeluju u razvoju programa za zaštitu od *cyber* napada te međunarodni standardi i preporuke koje poboljšavaju sigurnost od *cyber* napada te funkcionalnost zračnog prometa u suočavanju s potencijalnim prijetnjama.

2. MOTIVI *CYBER* PRIJETNJI

Cyber prijetnja se može definirati kao bilo koji identificirani napor usmjeren na pristup, izvlačenje iz sustava, manipulaciju ili oštećenje integriteta, povjerljivosti, sigurnosti i dostupnosti podataka, aplikacija i političkih sustava bez zakonitog dopuštenja. Bilo kakav neovlašteni pristup sustavima infrastrukture zračnog prometa smatra se *cyber* prijetnjom. Ovisno o određenom cilju zračnog prometa, *cyber* motivi mogu biti različite i široke prirode. Motivi *cyber* prijetnji se karakteriziraju prema izvorima i prema stupnju sigurnosti što itekako određuje metode kojima se određene službe zračnog prometa služe u borbi protiv *cyber* napada. Da bi se određena *cyber* prijetnja uklonila što brže i što bolje, sami motivi *cyber* prijetnji predstavljaju možda i najvažniji korak.

2.1. Izvori i podjela cyber prijetnji

Cyber prijetnja može biti namjerna ili nenamjerna, ciljana ili ne-ciljana, a može doći iz različitih izvora, uključujući: strane zemlje koje se bave špijunažom i informacijskim ratovanjem, kriminalce, hakere, autore virusa i nezadovoljnih zaposlenika i poduzetnika koji rade unutar određene organizacije. Nenamjerne prijetnje mogu biti uzrokovane nepažljivim ili neobučenim zaposlenicima, nadogradnjama softvera, postupcima održavanja i kvarovima opreme koji nenamjerno ometaju računalne sustave ili oštećuju podatke. Nedovoljno obučeno osoblje u službama zračnog prometa može biti veliki problem jer osobe ili organizacije koje imaju cilj izvršiti *cyber* napad na sustave zračnog prometa za primarnu metu izabiru upravo njih. Također službe koje su zadužene za ažuriranje sustava u zračnom prometu moraju adekvatno rukovati računalnim sustavima i paziti da prilikom ažuriranja sustava ne dođe do podmetanja bilo kakvog *cyber* virusa, [1].

Namjerne prijetnje uključuju ciljane i neciljane napade. Ciljani napad predstavlja djelovanje skupine ili pojedinca na određeni dio infrastrukture u zračnom prometu. Prilikom toga, pojedinci ili organizacije odrede fokus na jedan dio infrastrukture sustava zračnog prometa koji svojim daljnjim djelovanjem utječe na sve ostale sustave zračnog prometa pri čemu je sami izvor *cyber* napada teško odrediti. Neciljani napad pojavljuje se kada je cilj napada neodređen, a to može biti virus, crv ili zlonamjerni softver objavljen na internetu bez određenog cilja. Neciljani napad najčešće rezultira time da pojedinci željni popularnosti ili dokazivanja ostavljaju zlonamjerne softvere ili viruse pri čemu zračni promet zbog svoje kompleksnosti pruža sami izazov.

Najčešće identificirana prijetnja koja je ujedno i najopasnija je „*insider*" - netko tko ima ovlašteni i legitiman pristup sustavu ili mreži. Drugi neprijatelji kao što su skupine organiziranog kriminala ili terorističke grupe podvrgnute željenom cilju, mogu iskoristiti „*insidere*“ (npr. nezadovoljni zaposlenik ili zaposlenik pod prijetnjom) ili mogu iskoristiti zaposlene osobe bez njihovog znanja (uzimajući nekoga s ovlaštenim mrežnim pristupom za umetanje diska koji sadrži skrivene kodove ili skrivene viruse). Međutim, unutarnje prijetnje mogu se otkriti i spriječiti organizacijskim (pravila), logičkim (autentifikacija) i fizičkim (ograničeni pristup službene kartice) kontrolama.

Svaki od navedenih načina *cyber* prijetnji mogu biti povezani, međusobno ovisiti jedan o drugom te ovisno o motivu i namjeri, mogu nastati jedan iz drugog. Važno je napomenuti da prijetnja može biti kombinacija *cyber* i fizičkog napada, primjerice fizički upad u zemaljsku infrastrukturu i modifikacija softverskog koda koji je ugrađen u infrastrukturu čine namjerni *cyber* i fizički napad. Kada ovlašteno osoblje ne slijedi proceduru provjere infrastrukture, a infrastruktura generira i prenosi podatke koji ugrožavaju sigurnost sustava, radi se o *cyber* i nenamjernom fizičkom napadu, [1].

Porastom korištenja sve sofisticiranijih računalnih sustava došlo je i do sve veće opasnosti od *cyber* napada, pogotovo kad je u pitanju špijunaža stranih država i krađa povjerljivih podataka. Budući da je opasnost od terorizma danas na vrhuncu, zbog nacionalne sigurnosti glavni prioritet u vezi *cyber* napada su strane države kojima je računalna tehnologija najbrži put do povjerljivih podataka. Mnoge zračne luke se okreću prema izvorima *cyber* napada unutar vlastite mreže, bazirajući se na takozvane „*insidere*“. Budući da je avijacija mjesto gdje svaka informacija ima gotovo identičnu važnost i gdje svakodnevno prođe ogroman broj ljudi, mreža otkrivanja izvora mogućih *cyber* napada puno je veća nego prije.

2.2. Razine cyber prijetnji prema stupnju sigurnosti

Cyber prijetnje se prema motivaciji mogu podijeliti na pet osnovnih razina te svaka od njih zbog svoje kompleksnosti zahtijeva određene mjere sigurnosti. Budući da se zračni promet kao opširno područje mora boriti istovremeno protiv svih *cyber* prijetnji, definirani su prioriteti prema razinama. Na slici 1 može se vidjeti interakcija pet razina *cyber* prijetnji uz koje se vide i razine pripremljenosti na određenu *cyber* prijetnju, [1].

Prvoj razini pripadaju tradicionalni hakeri, pojedinci koji većinu vremena provode na internetu. Svojim djelovanjem u cilju prikazivanja vlastitih sposobnosti čine *cyber* napade koji su na najnižoj listi prioriteta zbog toga jer nemaju određenu metu a uz to imaju ograničene resurse i ograničeno znanje. Njihovi računalni sustavi nisu dovoljno razvijeni da naprave ozbiljnu štetu. Njihova meta su organizacije koje nemaju dobro razvijen sustav zaštite te su samim time ranjive putem interneta gdje ovakvi hakeri i djeluju.

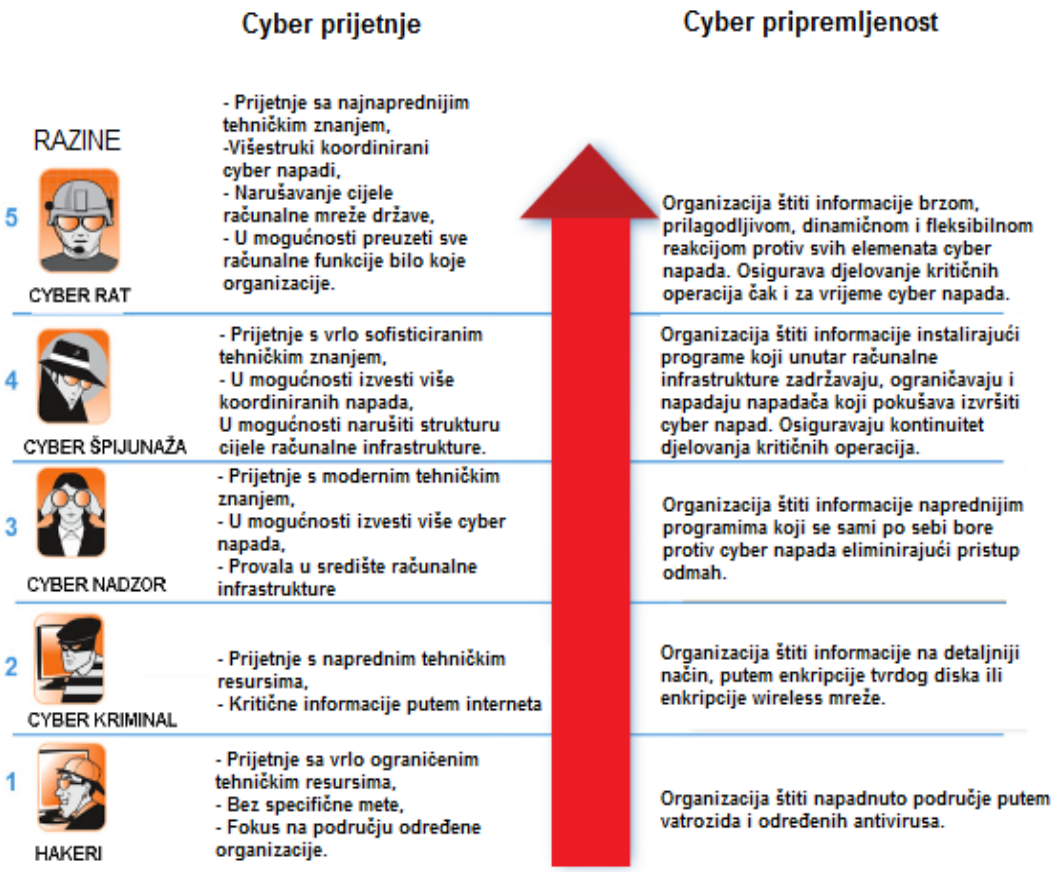
Drugoj razini pripadaju *cyber* lopovi koji putem svojih računalnih sustava pokušavaju steći važne informacije kojima bi mogli ugroziti neke od podsustava zračnog prometa. Također pokušavaju doći i do brojeva kreditnih kartica te vlasničkih poslovnih planova. *Cyber* lopovi ponajviše rade u skupinama sa razvijenijim i sofisticiranijim računalnim sustavima u odnosu na hakere. Zaštitu na ovoj razini predstavlja kontrola podataka unutar cijele organizacije putem korištenja tehnika kao što je šifriranje tvrdog diska.

Treća razina odnosi se na *cyber* nadzor u kojem napadači ciljaju ući duboko unutar organizacije putem određenih softvera, virusa i aplikacija koje su nevidljivi sustavima zaštite. Oni vrše iznenadne napade koji mogu biti u bilo kojem trenutku što predstavlja veliki problem sigurnosnim službama. Ono čime se ističu napadači na ovoj razini je viša stručnost pomoću koje mogu pokrenuti više napada unutar određene organizacije. Posljedice od napada na ovoj razini mogu biti vrlo ozbiljne, raspon se kreće od djelomičnog ili potpunog gubitka vlasničkih informacija u službi upravljanja zračnim prometom, neovisno o tome da li su posljedice napada

namjerne ili nenamjerne. Zaštita od *cyber* nadzora na ovoj razini zahtijeva kontinuirani i jaki nadzor unutar cijelog sustava zračnog prometa.

Na četvrtoj razini nalaze se *cyber* špijunske jedinice u čijem se sastavu nalaze visoko sofisticirani protivnici koji su sposobni za montažu i provođenje više koordiniranih napada. Njihov cilj je ulaz duboko u infrastrukturu organizacije gdje mogu koristiti visoko razvijene i isplanirane sustave za krađu najosjetljivijih informacija ili za onemogućavanje cijelog sustava. *Cyber* špijunskim jedinicama pripadaju obično jako financirane skupine kojima su dostupni i neki od najrazvijenijih računalnih sustava. Zaštita od *cyber* špijunskih jedinica zahtijeva jaku sigurnosnu arhitekturu cijelog sustava zračnog prometa koja može ugroziti akcije svih napadača u okviru informacijskog sustava infrastrukture zračnog prometa te osigurati kontinuitet provođenja kritičnih operacija.

Na petoj razini nalazi se i najopasniji mogući *cyber* napad koji se naziva *cyber* ratovanje. *Cyber* ratovanje čine najstručniji pojedinci spojeni u veliku mrežu koja je jako financirana te koristi najrazvijenije računalne sustave koje je gotovo nemoguće pronaći. Napadači na ovoj razini imaju neograničena sredstva za višestruke isplanirano kontinuirane i koordinirane napade. Zaštita od *cyber* napada zahtijeva pokretljivost, prilagodbu i fleksibilnost te maksimalnu koordinaciju više službi da bi se vremenski moglo što prije ući u trag cber skupinama koje čine *cyber* ratovanje. Isto tako u odjelu zaštite protiv *cyber* ratovanja moraju djelovati najstručniji računalni pojedinci koji će u međusobnoj koordinaciji dinamički preoblikovati operacije i time održati kontinuitet zaštite čak i kad je zračni promet pod stalnim napadima, [1].



Slika 1. Međusobna interakcija *cyber* prijetnji i pripremljenosti na *cyber* prijetnje

Izvor : [1]

Nažalost unutar ovih pet razina postoji i mnogo više *cyber* napada koji nisu jasno definirani nego mogu biti kombinacija više razina što dovodi do jako teške situacije u pogledu zaštite i sigurnosti. Pripremljenost u odnosu na takve napade postaje jako teška i kompliciranа budući da se napadači koji vrše *cyber* napad ne mogu jasno deklarirati prema razini *cyber* prijetnji. Ono što je važno napomenuti je to da se svakoj razini koja ima minimalne elemente više razine automatski suprotstavlja viša razina *cyber* pripremljenosti.

3. UTJECAJ *CYBER* NAPADA NA PODSUSTAVE ZRAČNOG PROMETA

Cyber napadi svojim djelovanjem ugrožavaju cijeli sustav zračnog prometa, no prema području djelovanja na zračni promet, mogu utjecati na zračne luke, prijevoznike u zračnom prometu i kontrolu zračne plovidbe. *Cyber* napadi ne ostavljaju iste posljedice na sve podsustave zračnog prometa što govori da svaki podsustav zračnog prometa djeluje drukčije u borbi protiv *cyber* kriminala. Budući da je zračni promet kompleksan i složen sustav, neophodno je da svi podsustavi zračnog prometa budu povezani u borbi protiv *cyber* napada.

Do danas je zračni promet kao zatvoreni sustav bio dobro izoliran od *cyber* napada. Kombinacija različitih faktora znači da se rizik od *cyber* napada znatno povećava kroz iduće načine, [2]:

- povećanje automatizacije i ovisnost o digitalnim sustavima,
- sve veća potreba za interoperabilnošću (komunikacija „zemlja-zrak“),
- premještanje u mrežnu središnju arhitekturu,
- povećanje korištenja zajedničkih komponenti više nego inače,
- miješanje postojećih i novih sustava,
- povećanje broja korisnika,
- povećanje sposobnosti *cyber* napadača.

Važno je povećati međusobnu povezanost i potencijalnu zajedničku upotrebu uobičajenih komponenti što znači da će države članice i operatori biti više ovisni jedno o drugom u cilju vlastite računalne sigurnosti. Najveća vjerojatnost je da će napadi biti usmjereni na ulazak preko slabih točaka mreže prije daljnjeg proslijeđivanja unutar mreže mreže. Pitanja o povjerenju i osiguranju su najvažnija budući da su sigurnost i osiguranje glavne značajke borbe protiv *cyber* napada [2].

3.1. Utjecaj *cyber* napada na zračne luke

Komercijalne zračne luke imaju područja koja imaju različitu razinu sigurnosti. Osigurana područja, sigurnosna područja za identifikaciju, područja zračnih operacija i sterilna područjima (gdje putnici čekaju ukrcaj u zrakoplov). Sigurnosna područja za identifikaciju i područja zračnih operacija obično uključuju područja za utovar prtljage, područja u blizini terminala i druga područja blizu parkiranih zrakoplova i objekata u zračnoj luci. Sva navedena područja pod utjecajem *cyber* napada mogu dovesti u pitanje funkcionalnost i sigurnost zračne luke.

Cyber napadi postaju glavna briga u pogledu sigurnosti zračnih luka zbog rastuće uporabe mobilnih aplikacija i hardvera. Osim tradicionalne računalne infrastrukture kao što su e-mail i internet, postoji još nekoliko potencijalnih ciljeva unutar područja internih operacija koji pod utjecajem *cyber* napada dovode zračnu luku u veliku opasnost. Čak su i male zračne luke jako ovisne o umreženim računalnim sustavima i stoga su jako ranjive na potencijalne *cyber* napade. *Cyber* prijetnje na zračne luke utječu putem brojnih načina kao što su, [3]:

- USB pogoni te prijenosna i netbook računala,
- bežične pristupne točke,
- razni USB uređaji (digitalne kamere, MP3 playeri itd.),
- čovjek „Trojan“ (napadači koji su prikriveni kao osoblje),
- optički mediji (CD, DVD, itd.),
- pametni telefoni,
- e-mail,
- društvene mreže,
- DDoS napadi,
- krađa podataka te unutarnje prijetnje i online prijevare.

Posljednjih godina svi najnoviji tehnološki uređaji su uobičajena pojava radnim mjestima gdje zaposlenici imaju visoko razvijene osobne uređaje. Opasnost od *cyber* napada se krije u povezanosti osobnih uređaja sa uređajima na zračnoj luci gdje se potencijalno mogu koristiti kako bi se prikupile povjerljive informacije ili unijeli virusi. Korištenje *wi-fi* mreže predstavlja veliki rizik od *cyber* napada prvenstveno jer mnoge zračne luke ne koriste adekvatnu zaštitu pa pristup povjerljivim podacima nije dovoljno zaštićen, [3].

Budući da kroz zračne luke svakodnevno prolazi mnogo ljudi, potencijalni *cyber* napad osim sigurnosti putnika i osoblja unutar zračne luke, neizravno utječe i na financije zračne luke gdje samo jedan *cyber* napad može prouzročiti ogromne financijske gubitke. Zbog visokog stupnja automatizacije na zračnim lukama, *cyber* napad direktno ugrožava funkcionalnost zračnih luka. Isto tako *cyber* napad može predstavljati ozbiljan problem zračnim lukama pri izradi planova i strategija u borbi protiv *cyber* kriminala zbog toga što se na njima radi svakodnevno te samo jedan propust znači „resetiranje“ svih planova. *Cyber* napad na zračne luke može utjecati i u pogledu reputacije gdje zračna luka propustom u zaštiti od *cyber* napada može izgubiti povezanost sa drugim zračnim lukama a samim time i još važnije, broj putnika.

3.2. Utjecaj *cyber* napada na prijevoznike u zračnom prometu

Prema istraživanjima 85% izvršnih direktora zrakoplovnih kompanija izrazilo je zabrinutost zbog opasnosti od *cyber* rizika. Kao i u drugim industrijama, prijevoznici u zračnom prometu su jako zabrinuti jer zbog *cyber* napada dolazi do krađe osjetljivih podataka od putnika ili samih prijevoznika. Dodanu prijetnju prijevoznicima u zračnom prometu predstavlja to što se tehnologija koristi se za razvoj povezanosti između sustava letačkih operacija sa osobljem na zemlji i sustavima zračnog prometa. Problem u borbi protiv *cyber* napada predstavlja i to što prijevoznici u zračnom prometu sve teže prate zahtjeve u pogledu sigurnosti i zaštite od *cyber* napada prilikom uporabe sve novijih tehnoloških sustava. Inovacije poput elektroničkih vrećica koje su popularne kod pilota i sustavi povezivanja putem Wi-Fi mreže su jako osjetljive na potencijalne *cyber* napade pogotovo jer mnogi prijevoznici u zračnom prometu nemaju definirani plan zaštite od *cyber* napada putem ovih inovacija. Ove inovacije znatno povećavaju broj priključaka što stvara više mogućnosti za potencijalno hakiranje sustava. Zbog potencijalnih prijetnji koje predstavljaju računalni sustavi, mora se adekvatno upravljati tako da prijevoznici u zračnom prometu usko surađuju s drugim službama, pružateljima hardvera i

softvera te drugih sudionika u zrakoplovnoj industriji. Budući da se povezanost zrakoplova u stvarnom vremenu i dalje razvija, pružajući informacije gdje i kada god je potrebno za optimizaciju operacija prijevoznika u zračnom prometu, *cyber* napadi time direktno čine još veću štetu svim prijevoznicima, [4].

Mnogi niskotarifni prijevoznici u zračnom prometu su u velikoj opasnosti od *cyber* napada budući da imaju zrakoplove sa starijim sustavima unutar zrakoplova. Unatoč tome mala je vjerojatnost da će niskotarifni prijevoznici u zračnom prometu biti suočeni sa *cyber* prijetnjama zbog toga što prevoze manji broj putnika što za napadače ne predstavlja izazov poput napada na velike kompanije. Najveći utjecaj *cyber* napada na prijevoznike u zračnom prometu odnosi se financije prijevoznika. U svakom slučaju, uspjeli *cyber* napad prouzrokuje veliku financijsku štetu prijevoznicima u zračnom prometu tako što velike kompanije moraju uložiti jako mnogo da bi se provele adekvatne mjere zaštite od *cyber* napada dok niskotarifni prijevoznici zbog nerazvijenih sustava dolaze na sami rub bankrota.

3.3. Utjecaj *cyber* napada na kontrolu zračne plovidbe

Cyber napadi na kontrolu zračne plovidbe mogu dovesti do velikih katastrofa. Neovlašteni pristup širokoj mreži računalnih i komunikacijskih sustava koje koriste kontrole zračne plovidbe širom svijeta može dovesti do katastrofe u obradi i praćenju tisuća letova. Istraživanja pokazuju da postoje mnogi propusti u zaštiti od *cyber* napada prilikom pristupa sustavima kontrole i komunikacije u zračnom prometu sa računalnih sustava koji nisu direktno uključeni u kontrolu zračne plovidbe. Uspješan *cyber* napad na kontrolu zračne plovidbe može predstavljati vrlo ozbiljan problem kada se radi o, [4] :

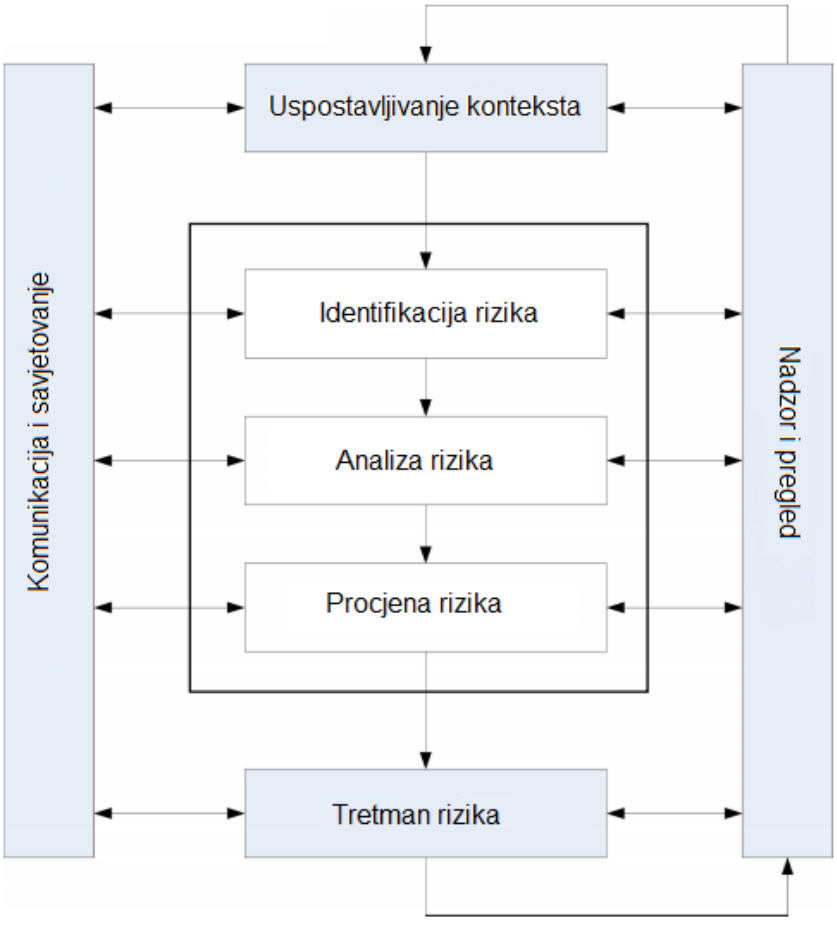
- otmici zrakoplova,
- krađi podataka zrakoplova,
- gubitku kontrole protoka zračnog prometa,
- sigurnosti putnika,
- sigurnosti zračne luke,
- krađi povjerljivih podataka.

Danas se u kontroli zračne plovidbe koristi ADS-B tehnologija koja u komunikaciji zrakoplova i kontrole zbog svoje sposobnosti pružanja šire pokrivenosti i poboljšanja situacijske kontrole zračnog prometa povećava kapacitet zračnog prometa. Međutim, kako se ADS-B tehnologija zemaljske stanice oslanjaju na spektar od 1090 MHz za primanje ADS-B poruka iz zrakoplova, komunikacija između zemaljske stanice i zrakoplova može biti zaglavljena generiranjem smetnji signala u blizini zemaljske stanice. ADS-B tehnologija trenutno ne zahtijeva provjeru autentičnosti u komunikaciji pa je moguć prijenos lažnih informacija ili se poruke emitirane iz legitimnih izvora mogu modificirati putem snažnih signala. U budućnosti komunikacijski, navigacijski i nadzorni (CNS) i ATM sustavi postaju sev ovisniji o digitalnoj tehnologiji što će jos više otežati borbu protiv *cyber* napada, [1].

4. METODOLOGIJA PROCJENE *CYBER* RIZIKA U PODSUSTAVIMA ZRAČNOG PROMETA

Metodologija procjene rizika u podsustavima zračnog prometa ovisi o mnogim parametrima koji od kojih je poželjno dobiti što više informacija. Ona je sastavni dio standardnog procesa upravljanja rizicima te omogućuje službama zračnog prometa da učinkovito prepoznaju, procijene i liječe rizik. Pojam „rizik“ se odnosi na bilo kakvu mogućnost da bilo koji dio sustava zračnog prometa bude izložen napadu. Analiza rizika sasvim sigurno pomaže kod određivanja odgovarajućeg sigurnosnog proračuna i smjera kojem sustav zračnog prometa teži. Kod ovog postupka iznimno je važno prvo utvrditi kontekst za procjenu rizika što uključuje definiranje samog opsega te identifikaciju imovine koja je potencijalno u opasnosti.

Identifikacija, analiza i procjena rizika zajedno čine i obuhvaćaju program procjene rizika u procesu upravljanja rizicima. Kao dio procesa analize rizika, komunikacija, savjeti i angažiranje dionika unutarnje i vanjske organizacije ključni su za identifikaciju, analizu i praćenje rizika. Kontrole koje osiguravaju da proces procjene rizika i dalje djeluje učinkovito temeljno čine detaljan nadzor i pregled svih dijelova sustava. Proces metodologije procjene rizika može se vidjeti na slici 2.



Slika 2. Proces upravljanja rizicima

Izvor: [1]

4.1. Identifikacija, analiza i procjena *cyber* rizika

Prvi korak u identifikaciji *cyber* rizika je prijava bilo kakve sustavne aktivnosti koja odstupa od norme. Aktivnosti kao što su usporenost sustava i osvježavanje podataka, nepotpune i neprimjerene informacije, kontrole (npr., linkova, pop-up prozora, ulazne okvira) na web stranici i preusmjeravanje na sumnjive nazive domena od strane korisnika čine rizik od *cyber* napada. U identifikaciji *cyber* rizika prvenstveno treba pogledati detaljno mrežne aktivnosti koje čak i osposobljeni stručnjaci za kibernetiku teško primjećuju kao što su povezivanja s IP adresama, skeniranje priključaka i razne sigurnosne usluge na mreži. Indikatori koji mogu upozoriti na bilo kakvu nepravilnu radnju u sustavu, mogu se postaviti na softvere i time upozoriti IT osoblje ili drugo odgovorno osoblje na nepravilnost.

Otkrivanje *cyber* prijetnje može biti učinkovitije ukoliko se u sve komponente računalnih sustava ugrade softveri za otkrivanje virusa i zlonamjernih programa. Bilo kakvo djelovanje na području sustava gdje se nalaze osobni podaci, financijski podaci, podaci o poslovanju, može se smatrati potencijalnom *cyber* prijetnjom. Otkrivanje *cyber* napada i primjena određenih protumjere je velik, ali kritičan zadatak. Osoblje kojem je povjereno ispunjavati ranije definirane uloge treba sudjelovati u najvećoj mjeri u kojoj su tehnički sposobni te prilikom *cyber* treninga imati na umu odgovornost koja im je dana u otkrivanju *cyber* prijetnji, [5].

Prilikom otkrivanja *cyber* prijetnji važno je odrediti stvari početna područja na kojima će se temeljiti otkrivanje *cyber* prijetnji i područja koja će poboljšati otkrivanje *cyber* prijetnji, a podjela se može vidjeti u tablici 1, [4].

Tablica 1. Područja identifikacije *cyber* prijetnji

Temeljna područja prilikom identifikacije cyber prijetnji	*Područja koja pospješuju identifikaciju cyber prijetnji*
Određivanje i razvoj učinkovitih i mjerljivih polazišta	*Ulaganje u napredne stvari i napredne tehnologije*
Održavanje cyber edukacija i cyber treninga	*Integriranje i razvijanje strožih protokola*
Određivanje opsega i prvenstva korištenja sredstava za borbu protvi cyber rizika	*Izgradnja bolje i prilagodljivije obrane od cyber napada*
Unutarnja suradnja službi zračnog prometa	*Stalna nadogradnja temeljena na nedostatcima*
Angažiranje stručnjaka	*Vanjska suradnja*

Izvor : [4]

Analiza *cyber* rizika treba biti što preciznija da bi se potencijalni *cyber* rizik uklonio u što kraćem roku sa što kraćim posljedicama. To znači da svaka analiza *cyber* rizika mora uključivati plan koji će odrediti s kakvim se rizikom sustav zračnog prometa suočava, kolika je vjerojatnost da će se desiti *cyber* napad, kakve posljedice mogu prouzročiti *cyber* napadi te koliko je vremena i resursa potrebno da bi se eventualni *cyber* napad uklonio. Kvalitetna analiza *cyber* rizika u avijaciji može se opisati u idućih šest koraka, [7]:

- utvrđivanje utjecaja *cyber* napada na povjerljivost, integritet i dostupnost,
- identifikacija ciljeva *cyber* napada,
- klasifikacija napadačkih tehnika *cyber* napadača,
- klasifikacija tehničke težine izvedivosti *cyber* napada,
- razvoj napadačkih „stabala“,
- utjecaj *cyber* napada.

Kvalitetan rezultat analize *cyber* rizika dobije se ukoliko svih šest koraka bude planski i detaljno analizirano. Povjerljivost, integritet i dostupnost podataka u svim podsustavima zračnog prometa moraju biti maksimalno zaštićeni i nedostupni potencijalnim *cyber* napadačima. Također u analizi *cyber* rizika vrlo važno je odrediti koji su ciljevi *cyber* napadača, koji dijelovi u sustavu zračnog prometa su najviše izloženi i koji mogu ostaviti najveće posljedice da bi se maksimalno organizirale protumjere i metode zaštite. Budući da *cyber* napadi mogu biti izvedeni putem raznih tehnika, kvalitetna analiza bi značila određivanje što je više moguće napadačkih tehnika kako bi se pronašla najbolja rješenja u suočavanju sa *cyber* napadima. Nažalost identifikacija napadačkih tehnika najčešće dolazi nakon *cyber* napada.

Svaki *cyber* napad nosi određenu težinu izvodljivosti koju određuje stupanj sigurnosti zračnog prometa te količina resursa za borbu protiv *cyber* napada. Razvijeni softveri koje najčešće imaju najprometnije zračne luke predstavljaju napadačima veći izazov prilikom *cyber* napada, a samim time i veću težinu tehničke izvedljivosti. Razvoj „napadačkih stabala“ znači uzimanje u obzir svih napadačkih tehnika da bi se što bolje izvršila procjena *cyber* rizika. „Napadačka stabla“ usko su povezana sa provjerama sigurnosti, performansama sofvtera i sistemskim kapacitetima. Nažalost analiza *cyber* rizika na temelju „napadačkih stabala“ većinom je temeljena na literaturi zbog nepredvidljivosti *cyber* napada i resursima koje koriste u stvarnosti. Utjecaj *cyber* napada može ostaviti različite posljedice koje su katerigorizirane prema skali između 1-5 pri čemu *cyber* napad kategorije 1 ima utjecaj sa razornim posljedicama dok *cyber* napad kategorije 5 ima utjecaj sa vrlo malim posljedicama, [7].

Procjena utjecaja *cyber* rizika je najteži korak u analizi *cyber* rizika jer se svodi na pretpostavke i pouke iz *cyber* napada koji su se ranije dogodili. Procjenu utjecaja *cyber* rizika određuju sigurnosni stručnjaci i IT stručnjaci na području zrakoplovstva. Procjena *cyber* rizika uključuje ispitivanje svih mogućih prijetnji i ranjivosti, ponajviše sa ljudskom prijetnjom koja može biti izvedena na mnogo načina. Pri procjeni *cyber* rizika uzimaju se u obzir i moguće posljedice koje određeni *cyber* rizik nosi te vjerojatnost nastanka *cyber* prijetnji. Procjena *cyber* rizika u suštini je usko povezana sa praćenjem i pregledanjem svih podsustava zračnog prometa, međusobnom komunikacijom i konzultacijama podsustava zračnog prometa te suradnjom u odnosu prema potencijalnom *cyber* riziku.

4.2. Razine posljedica javljanja *cyber* rizika

Posljedice javljanja *cyber* rizika imaju širok raspon te mogu utjecati na svaki dio sustava zračnog prometa. Posljedice javljanja *cyber* rizika trebaju biti shvaćene maksimalno što znači da traže ozbiljnu pažnju jer one direktno ugrožavaju poslovanje zračne luke a samim time i povećanje troškova. Budući da je vrijeme ključan faktor prilikom suočavanja sa *cyber* rizicima, ono na što treba obratiti pozornost su prihvatljivi rizici i neprihvatljivi rizici zbog toga što do određene reakcije na *cyber* napad brzo treba razmotriti što je prihvatljiv rizik a što ne.

Prihvatljiv rizik znači da potencijalni *cyber* napad neće utjecati na sigurnost dijelova zračnog prometa dok neprihvatljiv rizik znači da sigurnost svih dijelova zračnog prometa dovedena u pitanje. U svemu tome, najvažnija je izloženost osoblja zračne luke u odnosu na posljedice javljanja rizika zbog toga što većina *cyber* napada može ozbiljno narušiti privatnost osoblja krađom osobnih podataka ili hakiranjem bankovnih računa. S obzirom da je sigurnost osoblja i civila najvažnija u zračnom prometu, prioritet pri suočavanju sa posljedicama *cyber* rizika svakako treba biti zaštita osoblja i civila na svakoj razini.

Zbog svoje širine i učinka na zračni promet, razine posljedica se dijele na pet razina u kojima djeluju na posadu, zrakoplove, službe zračnog prometa, financije, usluge zračne luke i reputaciju zračne luke. Svaka od pet razina kategorizirana je određenim uvjetima kakav pristup u suočavanju će se primijeniti, [1]. Na slici 3. mogu se vidjeti razine posljedica javljanja *cyber* rizika te njihovo djelovanje i učinak na određene dijelove sustava zračnog prometa.

Kategorije	OPERANTI		FINANCIJE	PRUŽANJE USLUGA	REPUTACIJA
	Utjecaj na posadu i Putnike	Utjecaj na ATM sustav			
Katastrofalan rizik 1	Više smrtnih slučajeva zbog sudara s drugim zrakoplovim, preprekama ili terenom	Nemogućnost održavanja bilo koje usluge	Financijski gubitak veći od 200 milijuna ili insolventnost gdje je potrebna državna potpora	Nemogućnost održavanja bilo koje usluge	Nepopravljiva šteta u odnosima s većinom od ključnih dionika (vlasnika, kupaca, zaposlenika, javni, dobavljači)
Veliki rizik 2	Veliko smanjenje u sigurnosnim granicama Mali broj ozbiljnih i fatalnih ozljeda ozbiljan stres zrakoplovnom osoblju	Nemogućnost da se dobije bilo koji stupanj usluge (uključujući i mjere za nepredviđene situacije) unutar jednog ili više sektora zračnog prostora za značajno vrijeme.	Financijski gubitak , tako da je potrebno odobrenje odbora	Nemogućnost da se dobije bilo koji stupanj usluge.	Manje pružanje usluga od većine ključnih dionika
Srednji rizik 3	Značajno smanjenje granica sigurnosti	Ozbiljno ugrožena sposobnost da pružaju uslugu unutar jednog ili više sektora zračnog prostora bez upozorenja za značajno vrijeme.	Financijski gubitak, tako da je potrebno odobrenje CEO.	Ozbiljno ugrožena sposobnost da pružaju uslugu	Manje pružanje usluga od većine dionika
Mali rizik 4	Blago smanjenje granica sigurnosti	Narušen a sposobnost za pružanje usluga unutar jednog ili više sektora zračnog prostora bez upozorenja za značajno vrijeme.	Financijski gubitak, tako da je potrebno odobrenje delegata.	Umanjena sposobnost za pružanje usluga	Povremene pritužbe ključnih dionika koje zahtijevaju dodatnu pozornost da se postigne zadovoljavajući rezultat.
Nezamjetan rizik 5	Potencijalne neugodnosti	Nema učinka na sposobnost za pružanje usluga u kratkom roku , ali se situacija treba pratiti i pregledavati zbog potrebe da se primjenjuje neki oblik mjera za nepredviđene situacije	Financijski gubitak koji se može upravljati unutar određene grane	Zanemariv utjecaj na sposobnost za pružanje usluga.	Izolirani prigovor od strane pojedinih dionika koji se može upravljati na zadovoljavajući ishod dnevnog posla

Slika 3. Posljedice javljanja *cyber* rizika

Izvor: [1]

4.3. Procjena vjerojatnosti nastanka *cyber* rizika

Uz navedene razine posljedica od rizika, prilikom suočavanja sa potencijalnim *cyber* rizikom potrebno je obratiti pozornost vjerojatnost nastanka *cyber* rizika. Najveći prioritet će imati rizici za koje je vjerojatno da će nastati unutar jednog sata dok nešto manji prioritet imaju

rizici za koje je vjerojatno da će se desiti između nekoliko sati do unutar jednog dana, zatim prioritet imaju rizici kojima je vjerojatnost pojave između nekoliko dana do unutar jedne godine pa rizici kojima je vjerojatnost pojave između jedne godine i pet godina, rizici kojima je vjerojatnost pojave između pet godina i pedeset godina jednom te na kraju rizici kojima je vjerojatnost pojave jednom ili nijednom unutar 50 godina, [1].

To znači da postoje i varijacije koje označavaju da je moguće i da najmanji rizik može biti prioritet ukoliko je vjerojatnost pojave unutar jednog sata u odnosu na veći rizik kojem je vjerojatnost pojave između pet godina i 50 godina. *Cyber* rizici koji imaju oznaku „A“ označavaju rizike koji ostavljaju najveće posljedice dok *cyber* rizici koji imaju oznaku „D“ označavaju rizike koji ostavljaju najmanje posljedice na podsustave zračnog prometa. Kao kombinacija posljedica javljanja rizika i vjerojatnosti pojave rizika, postoji šest vremenskih kriterija u kojima se može pojaviti *cyber* napad. Isto tako ti vremenski kriteriji određuju i načine i sredstva kojima će se pristupiti u eliminaciji *cyber* rizika, [1]. Međusobni odnos posljedica javljanja *cyber* rizika i vjerojatnosti pojave *cyber* rizika može se vidjeti na slici 4.

Kriterij vjerojatnosti		Kriterij posljedica				
Vjerojatnost da će se dogoditi cyber napad:		Katastrofalne 1	Velike 2	Srednje 3	Male 4	Nezamjetne 5
1	Unutar jednog sata	A	A	A	A	C
2	Između nekoliko sati do unutar jednog dana	A	A	A	B	D
3	Između nekoliko dana do unutar jedne godine	A	A	B	C	D
4	Između godine i 5 godina	A	B	C	C	D
5	Između 5 godina i 50 godina	A	B	C	D	D
6	Manje vjerojatno unutar 50 godina	B	C	D	D	D

Slika 4. Odnos posljedica javljanja *cyber* rizika i vjerojatnosti nastanka *cyber* rizika

Izvor : [1]

5. PROVOĐENJE PREVENTIVNIH MJERA I METODE ZAŠTITE

U kontekstu konvencije o međunarodnom civilnom zrakoplovstvu ("Čikaška konvencija") službe u zračnoj plovidbi su dio državne obveze, a države moraju čuvati bitne interese nacionalne sigurnosti te u mnogim slučajevima moraju ispuniti određene zakonske zahtjeve, obveze i specifične postupke vezane uz zaštitu računalne infrastrukture zračnog prometa. Najveću važnost u pogledu *cyber* sigurnosti u zračnom prometu imaju integritet podataka i osiguranje informacija. Stoga je važno razumjeti zahtjeve za osiguravanje podataka i informacija kao i mjere i strategije koje se mogu poduzeti u tom pogledu.

Upravljati zračnim prometom znači biti u stanju procijeniti utjecaj sigurnosti i nedostatak sigurnosti na performanse mrežnog sustava zračnog prometa. To uključuje izvođenje analiza troškova te uvođenje ili odsutnost sigurnosnih funkcija. Potrebno je odrediti odgovarajuće politike, postupke i procese. Potrebno je uspostaviti mehanizme za otkrivanje *cyber* prijetnji i unaprijeđenje alata koji su potrebni za procjenu i ublažavanje prijetnji. Potreban je pristup koji koristi standardizirane postupke ublažavanja svake *cyber* prijetnje pri minimalnom riziku, temeljenim na utvrđenim pravilima i postupcima, [5].

5.1. Područja provođenja preventivnih mjera

Početni korak za smanjenje *cyber* rizika je identificirati prijetnje koje prijete sustavima zračnog prometa te što prije zaštititi podatke i sustave koji bi mogli biti ugroženi takvim prijetnjama. Sljedeći je korak zaštititi podatake i sustave provođenjem protumjera koje smanjuju vjerojatnost uspješnog *cyber* napada. Ono što nije dobro je to da malo organizacija može provoditi sve potrebne protumjere istovremeno. Čak i ako je to moguće, najprije je potreban pristup na dio zračnog sustava koji ima najviši prioritet, a taj prioritet se treba utvrditi procjenom vjerojatnosti ranjivosti i stupnja utjecaja koji može imati uspješan *cyber* napad. Moderne zračne luke zahtijevaju kontinuirani, fleksibilan i prilagodljiv pristup pri procjeni ranjivosti da bi se provele što adekvatnije protumjere. Područja djelovanja protumjera podijeljena su na pet kategorija, gdje se tri kategorije dijele na podkategorije na kojima je iznimno važno provesti najbolje protumjere. Područja djelovanja protumjera i njihove podjele su, [5] :

- aerodromski računalni sustavi
  - IT infrastruktura
  - *End-Point* sistemi
  - industrijski kontrolni sistemi
  - Wi-Fi
  - Cloud servisi
  - GPS
- utjecaj ljudi
  - socijalno inženjerstvo
  - vlastiti računalni uređaj
  - mediji
  - *insider*

- pružatelji usluga
  - pružatelji usluga koji mogu pospješiti vjerojatnost *cyber* napada
  - pružatelji usluga koji sudjeluju u obrani protiv *cyber* napada
- putnici i ostali civili
- privatne i osjetljive informacije

Područja u kojima je priprema protiv cyber prijetnje najučinkovitija mogu se podijeliti na, [6]:

- nadogradnju sustava,
- komunikaciju unutar zračnog sustava,
- operativni dogovor.

5.2. Zaštita u službi upravljanja zračnim prometom

Zaštita u službi upravljanja zračnim prometom je glavna komponenta zaštite u zrakoplovstvu. Zabrinuta je za one prijetnje koje su usmjerene na izravno na sustav poput izravnih *cyber* napada ili napada gdje služba upravljanja zračnim prometom igra ključnu ulogu u prevenciji ili odgovoru na prijetnje usmjerene na druge dijelove zrakoplovnog sustava. Sadrži dva ključna područja:

1. **Samozaštita sustava službe za upravljanje zračnim prometom** koja se odnosi na sigurnost i otpornost fizičke infrastrukture, osoblje, informacije i komunikacijske sustave, infrastrukture i mreže službe za upravljanje zračnim prometom te komunikacijskih, navigacijskih i nadzornih sustava;

2. **Zajednička podrška** službe za upravljanje zračnim prometom zaštiti zrakoplovstva te civilnoj i vojnoj vlasti odgovornoj za nacionalnu sigurnost i obranu.

Prijetnje mogu biti usmjerene na zrakoplov ili pomoću njih na ciljeve na tlu. Objekti i sustavi službe za upravljanje zračnim prometom također mogu postati ciljevi prijetnji. Međunarodna dimenzija nameće ujednačenu i učinkovitu primjenu prikladnih mjera u cilju prevencije posljedica od *cyber* napada. To znači da služba za upravljanje zračnim prometom nije u mogućnosti sama donijeti rješenje problema nego mora odgovarati i postupati po određenim pravilima. Služba za upravljanje zračnim prometom mora podržavati nacionalnu sigurnost u pogledu identifikacije letova koji ulaze u nacionalni teritorij te pružiti određene informacije organizacijama protuzračne obrane. Planiranje nepredviđenih okolnosti je bitan dio cjelokupnog sigurnosni programa jer ima cilj vratiti sustav što je prije moguće na "normalno" da bi se spriječilo ponavljanje istog *cyber* napada, [7].

5.3. Razvoj *Cybersecurity* programa

Ključne komponente prilikom izrade *cybersecurity* programa uključuju, [5] :

- upravljanje,
- osposobljavanje,
- resurse,
- trenutne aktivnosti,

- rizike.

Upravljanje u *cybersecurity* programu obuhvaća zakone, propise, politike, standarde, specifikacije i postupke. Odnosi se na način kojim ljudi nadgledaju *cybersecurity* program. Upravljanje proizlazi iz strateške perspektive, ali vodi i utječe na dnevne aktivnosti određenih pojedinaca, ali i svih ostalih. Upravljanje obuhvaća zakonske zahtjeve i propise kojih se zračna luka mora pridržavati te politike koje zahtijevaju standarde i postupke koje treba slijediti. Kontrolira procese koji osiguravaju da podaci i softver zadovoljavaju kriterije zračne luke, ugovore i mehanizme nabave kako bi se dobila odgovarajuća vanjska podrška. Zajedno, ti elementi omogućuju podsustavima zračnog pometa da program *cybersecuritya* provode na dosljedan način koji je usklađen s cjelokupnim organizacijskim ciljevima, [5].

Osposobljavanje osigurava da viši rukovoditelji, menadžeri, osoblje, konzultanti i drugi shvate važnost *cybersecuritya* i vlastitu ulogu u zaštiti podataka i sustava zračne luke od *cyber* napada. Osposobljavanje je jedan od najvažnijih dijelova važan u programu *cyber* sigurnosti. Najčešće prijetnje se mogu spriječiti pružanjem kvalitetne obuke koja povećava svijest i potiče zaposlenika i ostalo osoblje budu na oprezu. Osposobljavanje se posebno pokazalo kao ekonomičan pristup postizanju osnovne razine zaštite *cyber* sigurnosti. Najbolja je praksa pružiti obuku svijesti o *cyber* kriminalu svakom novom zaposleniku uz godišnji seminar za obavljanje znanja. Vrste obuke kreću se prema potrebama određenih službi u zračnom prometu. Univerzalni trening za konfiguraciju hardvera i softvera u podsustavima zračnog prometa trebaju voditi stručnjaci koji planiraju cjelokupni plan *cyber* sigurnosti.

Cybersecurity program zahtijevaju odgovarajuću kombinaciju unutarnjih i vanjskih resursa kako bi suočavanje sa *cyber* prijetnjama bilo što učinkovitije. Razina i kombinacija potrebnih resursa znatno će se razlikovati ovisno o veličini zračne luke te njenom menadžmentu da koristi unutarnje osoblje u odnosu na vanjske konzultante. Korištenje vanjskih izvora nije preporučljiva opcija jer neke od potrebnih vještina i sposobnosti nisu potrebne cijelo vrijeme. Na jednom kraju zračna luka treba dostupne materijale kako bi imali besplatnu obuku i dijeljenje informacija uz instalaciju određenih softvera za zaštitu krajnjih točaka. Na drugom kraju spektra, zračna luka može trošiti dodatna sredstva na obuku konzultante i ostale vanjske suradnika. Kad su resursi u pitanju, glavne komponente su osoblje, ulaganja i vanjska podrška.

Najvažnija komponenta u *cybersecurity* programu je kontroliranje rizika. Kontrola rizika mora biti uvijek zadovoljena što znači da prilikom kontrole rizika nema mjesta ni najmanjoj pogrješci. Budući da pojam rizika čine vjerojatnost pojave rizika i posljedice koje eventualni rizik može ostaviti, postoji nekoliko komponenti koje sadrži kontrola rizika. Rizik uvođenja protumjera protiv *cyber* programa može se očitovati u, [5] :

- lažnom osjećaju sigurnosti,
- nedovoljnoj uočljivosti *cyber* prijetnji,
- prekomjernim reakcijama na prijetnje,
- zbunjenost pri visokoj stopi prometa,

- lošu analizu prethodnih programa,
- prevelikim i nepotrebnim troškovima ,
- prekomjernim informacijama.

5.4. Načelo zaštite od *cyber* napada

U zaštiti zračnog prometa pri borbi sa *cyber* prijetnjama, međunarodna metoda djeluje prema načelu *isplanirati-štititi-identificirati-reagirati*. Načelo koje se može vidjeti na slici 5., uključuje kvalitetan dizajn strategije i arhitekture mreže cijele organizacije što utječe na povećanje sigurnosti, osiguranje okretnosti i smanjivanje ukupnih troškova. Određivanje prioriteta informacijske sigurnosti te ulaganje u nove i stare sustave osnovna je zadaća načela u zaštiti od *cyber* napada. Tehnike za zaštitu moraju biti precizno i jasno određene što znači da moraju biti u stanju brzo se mijenjati i prilagoditi za svaku moguću prijetnju. Razvoj tehnologije i povećanje kapaciteta zračnog prometa zahtijevaju od službi da iskoriste nove tehnologije i implementiraju ih na svakoj mogućoj razini. Dok pojedini dijelovi sigurnosti moraju biti ugrađeni u određene sustave, rješenje može biti bilo koji dio sigurnosnog sustava unutar cijele organizacije. Kada se gleda u pogledu sigurnosti, sasvim sigurno je da uspjeh svake informacijske tehnologije ovisi o sposobnosti sljedećih dvaju dijelova načela - identifikacija i odgovor na *cyber* prijetnju.

Identifikacija zahtijeva strukturiran i centraliziran pogled cyber sigurnosti operativnog centra (SOC – *Security Operations Centre*) sastavljen od tima stručnjaka koji svojim znanjem drastično pomažu razvoju zaštite od *cyber* prijetnji. Sigurnosni operativni centar mora biti podržan od strane alata za analizu sastavljenih od protuprovalnih senzora za nadgledavanje koji su instalirani u cijelom sustavu. Takav način djelovanja pruža mogućnost da se prepozna bilo kakva ugroženost informacijskog sustava u zračnom prometu. Identifikacija predstavlja otkrivanje bilo kakvih neuobičajenih radnji u sustavima, kontinuirano praćenje protoka informacija u zračnom prometu, instalaciju antivirusa i softvera koji pospješuju detekciju *cyber* prijetnji te praćenje i nadgledanje osoblja, putnika i ostalih osoba koji mogu biti predmetom *cyber* prijetnje. Također ono što je vrlo važno za identifikaciju *cyber* prijetnji je to da osoblje mora biti kvalitetno obučeno zbog toga što se tehnologija razvija iz dana u dan a to znači i da se mreža potencijalnih *cyber* napada također razvija, [5].

Odgovor na *cyber* napad uključuje planiranje u kriznim situacijama, procedure i obuke koje omogućuju službama zračnog prometa da brzo i učinkovito odgovore na pojavu *cyber* prijetnji i time smanje mogući utjecaj na sigurnost poslovanja. *Cyber* sigurnost danas gotovo da ne postoji u programu tekućih programa obuke osoblja, a takvo znanje je uistinu potrebno za kontrolore zračnog prometa, tehničare i drugo osoblje koje bi time što lakše identificiralo potencijalnu opasnost. Glavne odlike odgovora na *cyber* prijetnje su, [5]:

- prikupljanje svih podataka i skeniranje sustava,
- analiza informacija dobivenih iz prikupljanja i skeniranja sustava,
- ograničenje sustava na temelju analiziranih informacija,
- koordinacija službi u cilju brzog eliminiranja *cyber* prijetnje.



Slika 5. Načelo zaštite od *cyber* napada

Izvor : [1]

6. MEĐUNARODNI STANDARDI I PREPORUKE ZA ZAŠTITU CIVILNOG ZRAKOPLOVSTVA OD *CYBER* NAPADA

Zbog povezanosti velikog broja ljudi koju zračni promet čini, mnoge države su se usuglasile da će zajedno pridonijeti borbi protiv svih vrsta opasnosti pa tako i *cyber* napada. Tako su doneseni određeni standardi kojih se svaka država mora pridržavati, a isto tako postoje i preporuke koje mogu pospješiti borbu protiv *cyber* kriminala. U razvoju *cyber* programa tako sudjeluju mnoge organizacije povezane sa zračnim prometom i samim time međusobnom koordinacijom i komunikacijom donose standarde i preporuke u cilju što kvalitetnije zaštite.

6.1. Organizacije uključene u program zaštite civilnog zrakoplovstva od *cyber* napada

Opasnost od *cyber* napada u civilnom zrakoplovstvu danas predstavlja ogroman problem pa se mnoge organizacije udružuju kako bi stvorile kvalitetan program kojim će opasnost od *cyber* prijetnji svesti na minimum. Budući da je zračni promet kompleksan i da se putem zrakoplova dnevno prevezu miljuni i milijuni ljudi, organizacije imaju težak zadatak implementirati standarde i preporuke koje će pospješiti borbu protiv *cyber* kriminala. Svaka od organizacija svakodnevno provodi ankete i istraživanja prikupljajući iskustva i informacije prema kojima će razviti i implementirati *cybersecurity* program.

U razvoju *cyber* programa sudjeluju, [9] :

- ICAO (International Civil Aviation Organisation),
- ECAC (European Civil Aviation Conference),
- EUROCONTROL,
- SESAR,
- FAA (Federal Aviation Authority),
- NextGEN (Next Generation Air Transportation System),
- ARINC,
- AEEC (Airlines Electronic Engineering Committee),
- A4A (Airlines for America),
- CEN (European Committee for Standardisation),
- ETSI (European Telecommunications Standards Institute),
- EUROCAE (European Organisation for Civil Aviation Equipment),
- RTCA SC 216,
- ICANN (Internet Corporation for Assigned Names and Numbers),
- IETF (Internet Engineering Task Force),
- DOT (Department of Transportation),
- JCG (The Joint (Industry) Coordination Group).

Područje djelovanja navedenih organizacija je široko rasprostranjeno što znači da djeluju u svim podsustavima zračnog prometa. Budući da je međusobna koordinacija i dijeljenje informacija ključan element u trajnoj borbi protiv *cyber* kriminala, sve organizacije bi trebale povisiti suradnju na razinu više zbog sve većih problema u međupolitičkim odnosima, a i prvenstveno jer je terorizam na vrhuncu. Program zaštite civilnog zrakoplovstva od *cyber*

napada danas u modernom svijetu znači jako puno zbog toga što broj putnika sve više raste a s time i razvoj tehnologije gdje *cyber* napadači imaju sve više prostora, [9].

6.2. Međunarodni standardi i preporuke

Ovaj podnaslov daje dodatne detalje o međunarodnoj organizaciji za standardizaciju (ISO – *International organization for Standardization*) 27000 seriji standarda i drugih sigurnosnih okvira kako slijedi:

- opis svakog od standarda ISO 27001 do ISO 27006,
- ISO 27005 standard koji osigurava smjernice za ISRM (*Information Security Risk Management*),
- *cybersecurity* u okviru nacionalnog američkog ministarstva trgovine, Institut za standarde i tehnologiju (NIST – *National Institute of Standards and Tehnology*).

Međunarodna organizacija za standardizaciju (ISO - *International Organization for Standardization*) u vezi sigurnosnih pitanja rezervirala je ISO 27000 serije standarde. ISO 27001, izvorno objavljen u listopadu 2005. godine, omogućuje specifikaciju za sustav upravljanja sigurnošću informacija (ISMS - *Information Security Management System*). Prvenstvena zadaća norme je da se osiguraju zahtjevi za uspostavljenje, provođenje, održavanje i kontinuirano poboljšanje sustava za upravljanje sigurnošću informacija. Ono što se odnosi na donošenje zakona bi trebala biti strateška odluka pod utjecajem organizacijskih potreba i ciljeva, sigurnosnih uvjeta, organizacijskih procesa koji se koriste te veličine i strukture organizacije.

Norma ISO 27002, također objavljena u 2005. godini, donosi kodeks prakse za informacije sigurnosti i kratak osvrt na potencijalne kontrole i mehanizme kontrole, koje mogu biti provedene u skladu sa uputama predviđenim u okviru ISO 27001. Oba dokumenta su namijenjena da se koriste zajedno kako bi se nadopunjavali jedan sa drugim.

Norma ISO 27005 daje smjernice za informacije o sigurnosnom upravljanju rizicima u organizaciji, posebice podržava zahtjeve informacijske sigurnosti sustava upravljanja definirane od strane ISO 27001. ISO 27005 standard ne pruža niti preporučuje specifičnu metodologiju, ali omogućuje pregled procesa ISRM, uključujući procjenu, tretman, odobravanje, komunikaciju, nadgledanje i pregled rizika.

Okvir za poboljšanje kritične infrastrukture *cyber* sigurnosti je izrađen od strane *US Commerce Department's National Institute of Standards and Technology* (NIST), te je pušten u veljači 2014. godine. On ne predstavlja nikakav novi standard ili koncept nego iskorištava postojeće *cyber* sigurnosne prakse koje su razvijene i usavršene od strane drugih organizacija, ne ograničavajući, ali uključujući ISO. Okvir predstavlja rizik baziran na sastavljanju smjernica koje mogu pomoći organizacijama utvrditi, provoditi, te poboljšati *cyber* sigurnosne postupke, te stvara zajedničku taksonomiju za unutarnju i vanjsku komunikaciju *cyber* sigurnosnih pitanja, kao i mehanizam za procjenu koji omogućuje organizacijama da se utvrdi njihova trenutna sposobnost za sigurnost, te plan za održavanje njihove sposobnosti. Okvir je iterativan

model koji je dizajniran da se razvije i prilagodi promjenama u prijetnji sigurnosti, uključujući nove procese i tehnologije.

Tri ključna elementa u okviru mehanizma procjene su : temelj, implementacija razina te profil. Ono što čini temelj su standardizirane sigurnosne aktivnosti, željeni rezultati te primjenjive napomene. Temelj se sastoji od pet funkcija koje se mogu izvoditi istovremeno, [1]:

- identificiranje,
- zaštita,
- otkrivanje,
- odgovaranje,
- obnavljanje.

Implementacija razina koristi se za stvaranje konteksta unutar kojeg organizacije mogu bolje razumjeti kako se njihove trenutne sigurnosne mogućnosti suprotstavljaju karakteristikama opisanim u NIST. Profil kao aspekt okvira priznaje da različite industrije i organizacije imaju različite poslovne potrebe, operativne modele, prohtjeve i dostupna sredstva za razvoj snažnog sigurnosnog programa. Profil omogućuje organizacijama uskladiti i poboljšati svoje sigurnosne prakse na temelju njihovih pojedinačnih okolnosti.

Preporuke u svrhu zaštite od *cyber* napada svedene su na 3 područja: nadogradnja računalnih sistema, sigurno povezivanje pojedinih službi te operativna reakcija na *cyber* napade. Preporuka je da se na svakom od navedenih područja izvedu uspješni simulirani *cyber* napadi da bi se otkrili nedostaci koje bi s vremenom rješavali. Nadogradnja računalnih sistema je neophodna jer primarni cilj službi u zračnom prometu je sigurnost putnika, a uz nadogradnju računalnih sistema sigurnost putnika je zasigurno na većoj razini. Sigurno povezivanje službi u zračnim lukama predstavlja područje u kojem komunikacija između službi mora biti maksimalno sigurna i povjerljiva jer bilo kakvo curenje informacija i podataka mogu iskoristiti hakeri ili teroristi čime bi opasnost od *cyber* napada bila jako izgledna. Operativne reakcije predstavljaju zadnje područje koje je iznimno važno, a govori o tome da na svaku minimalnu anomaliju u prethodna dva područja treba što brže i efikasnije eliminirati, tj. da odgovarajuće službe trebaju biti spremne na svaku operativnu reakciju u cilju suzbijanja *cyber* opasnosti, [1].

Također preporuke u cilju poboljšanja zaštite od *cyber* napada mogu se podijeliti na dva glavna područja, [10]:

- sigurnost zračne luke,
- sigurnost zrakoplova.

Poboljšanje sigurnosti zračne luke očituje se u boljem profiliranju putnika na nekim drugim čimbenicima osima nacionalnosti, rase i religije. Isto tako sigurnost se može poboljšati detaljnijim pregledom letačkog osoblja, izradom propusnica za osoblje na temelju biometrijskih podataka, detaljnijim pregledom pribora koji se koristi u zrakoplovu i zračnim lukama te implementacijom novih sigurnosnih skenera.

Poboljšanje sigurnosti zrakoplova očituje se ponajprije u zaštiti kokpita gdje je preporuka što bolje i kvalitetnije zaštititi vrata kokpita u zrakoplovu. Kvalitetne simulacije otmice zrakoplova i situacije kada je u zrakoplovu bomba preporuka su u poboljšanju sigurnosti zrakoplova. Bolja kontrola sigurnosti zrakoplova može se poboljšati korištenjem zaštitara na letu, boljom kontrolom deportiranih putnika, boljom kontrolom putnika nedoličnog ponašanja, razvojem računalnih sustava, što boljim i bržim oporavkom sustava nakon eventualnog pada sistema te sigurnosti u *cargo* odjelu, [10].

7. ZAKLJUČAK

Cyber prijetnje danas predstavljaju veliki problem za sigurnost svih podsustava zračnog prometa. Svakog dana tehnologija napreduje sve brže i brže a time opasnost od *cyber* napada nažalost sve više raste. Vrhunac opasnosti od terorizma je na snazi, a i političko-diplomatski ratovi nažalost postaju svakodnevnica. Zračni promet je za *cyber* kriminal idealno mjesto budući da je putem računalnih sustava najlakše pristupiti infrastrukturi i osoblju zračnog prometa. Budući da je sigurnost osoblja, putnika i ostalih osoba koje sudjeluju u zračnom prometu ljudi najveći prioritet, potrebno je stalno raditi na razvijanju novih programa koji će se kvalitetno i efikasno suprostaviti svakom obliku opasnosti, pa *cyber* napadima.

Motivi *cyber* prijetnji mogu bti različite prirode i zato sve službe u međusobnoj koordinaciji imaju zadatak implementirati nove programe *cyber* sigurnosti. Isto tako treba svakodnevno raditi na sortiranju izvora *cyber* prijetnji da bi se točno znalo koja protumjera će se upotrijebiti protiv određenog izvora *cyber* napada. Da bi *cybersecurity* program bio što kvalitetniji potrebno je dobro pznavati razine *cyber* prijetnji prema stupnju sigurnosti, a to znači da cijelokupno osoblje koje sudjeluje u zaštiti zračnog prometa treba biti stručno osposobljeno.

Utjecaj *cyber* prijetnji na podsustave zračnog prometa može biti katastrofalan. Sve službe koje djeluju u zračnom prometu, neovisno na podsustave moraju djelovati zajedno protiv *cyber* napada. Zračne luke trebaju inzistirati na implementaciji najrazvijenijih računalnih sustava bez obzira na cijenu zbog toga što će moći preusmjeriti pažnju na poslovanje dok bi se manji bavili borbom protiv *cyber* kriminala. Također zračne luke trebaju biti svjesne koliko štete može prouzročiti samo jedan uspješan *cyber* napad i prema tome postaviti veću zaštitu i snažnije prioritetena cijeli računalni sustav unutar zračne luke.

Prijevoznici u zračnom prometu moraju osigurati kvalitetnu zaštitu unutar zrakoplova kako bi se spriječilo bilo kakvo moguće ugrožavanje sigurnosti posade i putnika. Moraju razviti detaljan plan kojim će se prvenstveno direktno suočiti sa *cyber* prijetnjama a uz to i pomoći drugim službama u suzbijanju *cyber* kriminala. Kontrola zračne plovidbe sasvim sigurno ima najveću odgovornost u zračnom prometu i stoga moraju biti najviše zaštićeni od *cyber* napada. Ono što je sasvim sigurno je to da svakako trebaju imati najmodernije računalne sustave uz maksimalnu zaštitu budući da su odgovorni za živote mnogih ljudi. Također sve ostale službe moraju uključiti kontrolu zračne plovidbe i u svoj plan.

Metodologija procjene rizika upodsustavima zračnog prometa treba biti detaljnije obrađena te pružiti više informacija prilikom izrade *cybersecurity* programa. Treba voditi računa o procjeni vjerojatnosti nastajanja *cyber* rizika i mogućim posljedicama koje određeni rizik nosi. Razrada plana koji će sadržavati detaljne informacije o procjeni rizika znači bolju sigurnost u zračnom prometu. Stručnjaci koji se bave metodologijom procjene rizika trebaju biti aktivni u obuci osoblja kako bi što veći broj ljudi bio upoznat sa procedurama i primjerenim reakcijama u slučaju javljanja *cyber* rizika.

Provođenje preventivnih mjera i metoda zaštite treba biti brzo i efikasno budući da je vrijeme krucijalno pri javljanju *cyber* rizika. Potrebno je jasno razraditi područja u kojima će se primjeniti preventivne mjere i metode zaštite. Razvoj *cybersecurity* programa je kompleksan ali uz adekvatnu obuku izvediv zadatak. Potrebno je oformiti stručne timove koji će svaki sa svog područja složiti kvalitetan program. Baza pri razvoju *cybersecurity* programa mora bit načelo *isplanirati-štititi-identificirati-reagirati*. Svaki od ovih koraka mora efikasno i precizno izvršiti svoju zadaću da bi kompletan program zaštite uspio.

Organizacije uključene u razvoj *cybersecurity* programa moraju svakodnevno tragati za boljim i efikasnijim rješenjima. Provođenje istraživanja će dati rezultate pomoću kojih će se donijeti precizni standardi za borbu protiv *cyber* kriminala. Isto tako poboljšanje standarda može se izvršiti ukoliko službe zračnog prometa poštuju i preporuke koje su dane radi bolje obrane od *cyber* napada.

Rad na svakodnevnim analizama rizika i „vaganja“ mogućih posljedica od strane *cyber* napada moraju biti što efikasniji i precizniji. Da bi se postigla što veća sigurnost, neophodno je da konačna rješenja budu izričito točna jer mjesta pogreškama kad je u pitanju zračna luka, zapravo i nema. Svaka država bi trebala znati da borba protiv *cyber* napada u zračnom prometu nije izbor nego uvjet, uvjet o kojem ovisi mnogo toga, a prije svega ono najvažnije – SIGURNOST.

POPIS KRATICA

A4A	(Airlines for America) - Prijevoznici za Ameriku
AEEC	(Airlines Electronic Engineering Committee) - Komitet prijevoznika elektroničkog inženjerstva
ARINC	(Aeronautical Radio Incorporated)
CEN	(European Committee for Standardisation) - Europski komitet za standardizaciju
DOT	(Department of Transportation) - Odjel za prijevoz
ECAC	(European Civil Aviation Conference) - Europska konferencija civilnog zrakoplovstva
ETSI	(European Telecommunications Standards Institute) - Europski institut za telekomunikacijske standarde
EUROCAE	(European Organisation for Civil Aviation Equipment) - Europska organizacija za civilno zrakoplovnu opremu
EUROCONTROL	(European Organisation for Safety of Air Navigation) - Europska organizacija za sigurnost navigacije u zračnom prometu
FAA	(Federal Aviation Authority) – Federalna zrakoplovna nadležnost
ICANN	(Internet Corporation for Assigned Names and Numbers) - Upravni odbor za dodjelu imena i brojeva
ICAO	(International Civil Aviation Organisation) - Organizacija međunarodnog civilnog zrakoplovstva
IETF	(Internet Engineering Task Force)
JCG	(The Joint (Industry) Coordination Group)
NextGEN	(Next Generation Air Transportation System) – Nova generacija prijevoznih sustava u zračnom prometu
RTCA SC 216	(Radio Technical Commission for Aeronautic) - Radio tehnička komisija za aeronautiku
SESAR	(Single European Sky Air Traffic Management Research) - Zajedničko poduzeće za istraživanje o upravljanju zračnim prometom jedinstvenog europskog neba

POPIS LITERATURE

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

[2.] Industry Consultation Body: Regulatory Response to ATM Cyber-Security, ICB, www.icb-portal.eu, 10.09.2015.

[3.] Gopalakrishnan, K., Govindarasu, M., Jacobson, D.W., Phares, B.M.: Cyber security for the Airports, International Journal for Traffic and Transport Engineering, Vol 3, p. 365-376, 2013.

[4.] Aviation Perspectives: 2016 special report series: Cybersecurity and the airline industry, 12.08.2017.

[5.] Murphy, R.J., Sukkarieh, M., Haass, J., Hriljac, P.: Guidebook on Best Practices for Airport Cybersecurity, Transportation Research Board, Washington; 2015.

[6.] Air Traffic Control Association Cyber Security Comitee: Aviation Cyber Security White Paper Series Executive Summary: Forming a Strategic Initiative to Combat Modern Cyber Security Threats, ATCA, Alexandria, 2016.

[7.] EUROCONTROL: Guidelines for NSAs for the Development of the ANSP Oversight Process, Annex 6 – ATM Security Oversight, EUROCONTROL, Bruxelles, 2013.

[8.] Pantoja Viveros, C.A.: Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts, Master thesis, University of Tartu, Institute of Computer science, Tartu, 2016.

[9.] Centre for the Protection of National Infrastructure: *Cyber security in civil aviation*, CPNI, London, kolovoz 2012.

[10.] European Cockpit Association: The European Pilots perspective on improving aviation security - Secure skies, ECA, Bruxelles, 2014.

POPIS TABLICA

Tablica 1. Područja identifikacije cyber prijetnji 11

POPIS SLIKA

Slika 1. Međusobna interakcija cyber prijetnji i pripremljenosti na *cyber* prijetnje..... 6
Slika 2. Proces upravljanja rizicima 10
Slika 3. Posljedice javljanja *cyber* rizika 13
Slika 4. Odnos posljedica javljanja *cyber* rizika i vjerojatnosti nastanka *cyber* rizika..... 14
Slika 5. Načelo zaštite od *cyber* napada..... 19

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

Student/ica:

U Zagrebu, 6.9.2017

Tomislav Nikolić

(potpis)