Upravljanje kibernetičkim rizicima u zrakoplovstvu

Bogdan, Tihana

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

UPRAVLJANJE KIBERNETIČKIM RIZICIMA U ZRAKOPLOVSTVU

AVIATION CYBER RISK MANAGEMENT

Mentor: prof. dr. sc. Sanja Steiner

Komentor: Dajana Bartulović, mag. ing. traff.

Student: Tihana Bogdan

JMBAG: 0135254775

Zagreb, kolovoz 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 4. svibnja 2022.

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

ZAVRŠNI ZADATAK br. 6674

Pristupnik: **Tihana Bogdan (0135254775)**
Studij: Promet
Smjer: Zračni promet

Zadatak: **Upravljanje kibernetičkim rizicima u zrakoplovstvu**

Opis zadatka:

Uvodno opisati predmet istraživanja, postaviti cilj i kompoziciju rada, te specificirati izvore. Dati pregled međunarodne regulative i prakse zaštite civilnog zrakoplovstva. Prezentirati status kibernetičke zaštite civilnog zrakoplovstva sa statističkom analizom povezanih događaja. Specificirati i opisati preventivne mjere kibernetičke zaštite civilnog zrakoplovstva. Elaborirati inovativne sustave upravljanja kibernetičkom zaštitom u zrakoplovstvu. Zaključno rezimirati tematiku rada i trend daljnjeg razvoja. Specificirati korištenu literature I mrežne izvore.

Mentor:

prof. dr. sc. Sanja Steiner

Predsjednik povjerenstva za završni ispit:

SAŽETAK

Napredak tehnologije jedna je od glavnih značajki modernog zrakoplovstva. Iako je upravo zbog tehnologije prijevoz zrakom uvelike olakšan i unaprijeđen, zastupljenost tehnologije dovodi i do sve većeg broja kibernetičkih napada. Kako bi se kibernetički napadi prevenirali, kontinuirano se radi na mjerama zaštite civilnog zrakoplovstva, ali i inovativnim sustavima koji zajedno formiraju otpornu i pouzdanu kibernetičku zaštitu. S ciljem boljeg upravljanja kibernetičkim rizicima, provode se razna istraživanja, analize i ankete koji omogućavaju lakše definiranje vrsta kibernetičkih napada te profila napadača, odnosno cjelokupnog statusa kibernetičke zaštite civilnog zrakoplovstva te definiranje zaštitnih mjera. U radu je analiziran sustav upravljanja kibernetičkim rizicima u zrakoplovstvu.

Ključne riječi: kibernetički napadi; kibernetička zaštita; tehnologija; mjere kibernetičke zaštite; inovativni sustavi kibernetičke zaštite

SUMMARY

Technology advancement is one of the main characteristics of modern aviation. Although presence of technology makes air transport easier and improved, it also causes increased number of cyber attacks. In order to prevent cyber attacks, continuous efforts are made regarding civil aviation security measures and innovative systems which create more resilient and reliable cyber security. Different research, analyses and surveys are being conducted to ensure that cyber risks could be well-managed in the way that they define types of cyber attacks and attackers, which efficiently defines overall cyber security status and helps define security measures. Thesis analyses the management of cyber risks in aviation.

Keywords: cyber attacks; cyber security; technology; cyber security measures; innovative cyber security systems

SADRŽAJ

1. UVOD

Iako se zračni promet smatra najsigurnijom vrstom prometa, značajna sredstva se ulažu u održavanje razine sigurnosti civilnog zrakoplovstva. Kako bi se spriječila djela nezakonitog ometanja pojedinih sudionika zračnog prometa, provode se brojne zaštitne mjere.

Dio tih zaštitnih mjera uključuje i preventivne mjere vezane uz kibernetičke prijetnje. Sustavi koji se koriste u zrakoplovstvu, a podložni su kibernetičkim napadima, su brojni. Broj tih kritičnih sustava povećava se s napretkom tehnologije. Takav ubrzani razvoj tehnologija i njihova primjena omogućavaju lakši pristup informacijama, obavljanje poslovnih aktivnosti na daljinu, automatizaciju procesa i smanjenje troškova poslovanja, ali i uzrokuje veću ranjivost sustava zbog kibernetičkih napada. Ovaj rad opisuje vrste kibernetičkih prijetnji i napadača, ali i zaštitne mjere i sustave koji se koriste kako bi se sudionici zračnog prometa mogli uspješno obraniti od kibernetičkih napada.

Svrha ovog rada je opisati regulativu, trenutni status, mjere i postupke te inovativne sustave upravljanja kibernetičkim rizicima u zrakoplovstvu.

Rad je podijeljen u šest poglavlja. U prvom poglavlju iznesena su uvodna razmatranja. Drugo poglavlje obuhvaća zakonsku regulativu i praksu zaštite civilnog zrakoplovstva. Treće poglavlje opisuje status kibernetičke zaštite pomoću statistike objavljene od strane međunarodno priznatih agencija i organizacija. Četvrto poglavlje definira standardizirane preventivne mjere kibernetičke zaštite civilnog zrakoplovstva. U petom poglavlju navedeni su inovativni sustavi i projekti čija je svrha efektivna obrana zrakoplovstva od kibernetičkih napada. U posljednjem, šestom poglavlju prikazana su zaključna razmatranja.

2. MEĐUNARODNA REGULATIVA I PRAKSA ZAŠTITE CIVILNOG ZRAKOPLOVSTVA

Početak dvadesetog stoljeća predstavlja razdoblje izuzetno brzog razvoja zračnog prometa. Posljedica toga jest potreba za stvaranjem zakona koji bi regulirali promet zrakom. Već 1910. godine u Parizu je održana prva konferencija o međunarodnoj zračnoj regulativi [1]. Uslijedile su brojne druge, među kojima su najpoznatije Pariška konvencija iz 1919. godine značajna po načelu suvereniteta države nad zračnim prostorom iznad njezina teritorija, Varšavska konvencija iz 1929. godine kojom je definirano pitanje odgovornosti prijevoznika za osobnu i materijalnu štetu putnika, Montrealska konvencija iz 1999. godine koja je zamijenila Varšavsku konvenciju te Konvencija o međunarodnom civilnom zrakoplovstvu [2]. Konvencija o međunarodnom civilnom zrakoplovstvu, poznatija pod nazivom Čikaška konvencija, jest međunarodni ugovor sastavljen u Chicagu 7. prosinca 1944. godine koji u 96 članaka utemeljuje prava i obveze svih zemalja potpisnica u području civilnoga zrakoplovstva [3].

Navedene konvencije stvorile su temelj zračnog prava. Zračno pravo je sustav pravila koji uređuje pravni status zračnoga prostora, zračnu plovidbu i promet, pravni status zrakoplova i pravni režim u pojedinim zračnim prostorima [2]. Najvažnijim instrumentom međunarodnog zračnog prava smatra se upravo Čikaška konvencija koju su ratificirale 193 države što ju čini jednim od najratificiranijih multilateralnih ugovora [1]. Zračno pravo dijeli se na međunarodno i domaće, no međunarodna pravila imaju veće značenje [2]. Zračnim pravom definiran je širok spektar tema koje uključuju odgovornost prijevoznika, sigurnost putnika, regulacije vezane uz zrakoplove, zračne luke i prtljagu, onečišćenje zraka, vojno zrakoplovstvo, ali i zaštitu civilnog zrakoplovstva [1].

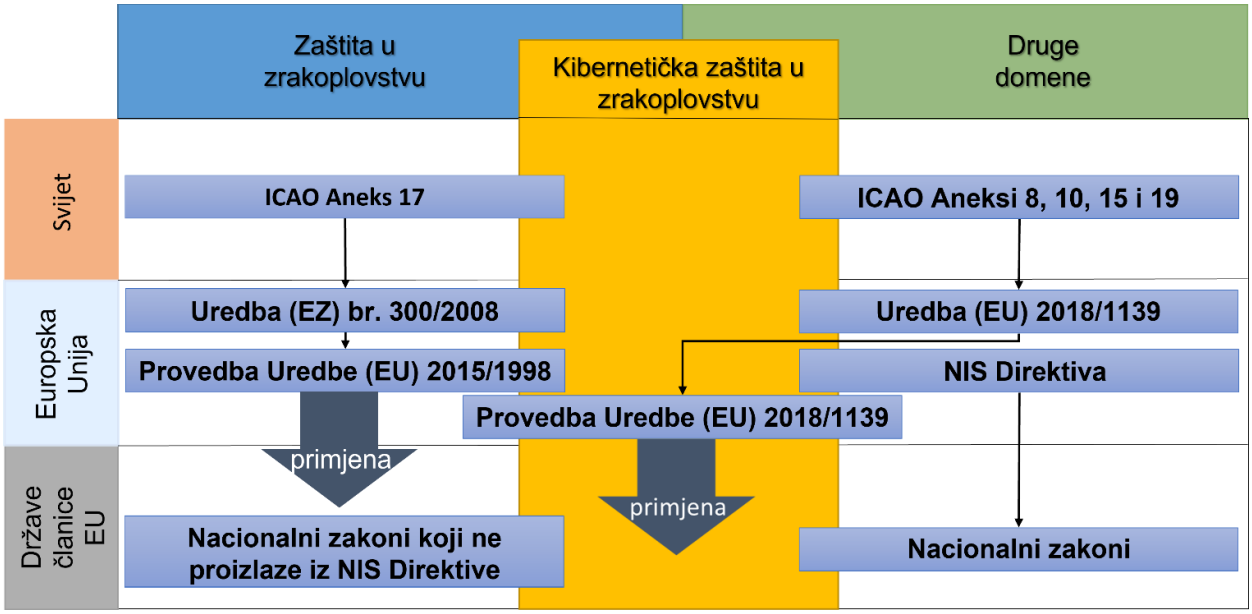
Zaštita civilnog zrakoplovstva uključuje i zaštitu informacija što je drugi naziv za kibernetičku zaštitu. Kibernetička zaštita je očuvanje raznih svojstava informacije kao što su povjerljivost, cjelovitost, dostupnost, autentičnost, odgovornost, neporecivost i pouzdanost [4]. S ciljem očuvanja kibernetičke zaštite nužno je primjenivati međunarodnu regulativu u kombinaciji s ljudskim i materijalnim resursima tj. u praksi.

2.1. Međunarodna regulativa

Organizacija međunarodnog civilnog zrakoplovstva (*International Civil Aviation Organization* – ICAO) specijalizirana je agencija Ujedinjenih naroda osnovana u Chicagu 1944. godine sa sjedištem u Montrealu. ICAO ima 193 države članice koje sudjeluju u donošenju Standarda i preporučenih praksi (*Standards and Recommended Practices* – SARPs) za civilno

zrakoplovstvo propisanih u 19 aneksa. Aneks 17 sadrži preventivne mjere zaštite civilnog zrakoplovstva uključujući konkretne mjere vezane za kibernetičke prijetnje [5]. Prema Aneksu 17 svaka država članica obvezna je osigurati da njeni operatori ili subjekti definirani u nacionalnom programu zaštite civilnog zrakoplovstva ili drugoj relevantnoj nacionalnoj dokumentaciji identificiraju svoje kritične sustave informacijske i komunikacijske tehnologije i podatke koji se koriste za potrebe civilnog zrakoplovstva te shodno tome razviju i prema potrebi provode mjere zaštite od nezakonitog ometanja [6].

Osim ICAO-a koji ima zakonodavnu ulogu na globalnoj razini, za definiranje zakonodavnog okvira kibernetičke zaštite u zrakoplovstvu zadužene su Europska Unija (*European Union* – EU) i pojedine države članice EU (slika 1). Europska unija, konkretno Europski parlament i Vijeće te Europska komisija, donose uredbe i direktive, a države donose zakone na nacionalnoj razini.



Slika 1. Zakonodavni okvir kibernetičke zaštite u zrakoplovstvu
Izvor: *[4]*

Od dokumenata EU, za zaštitu civilnog zrakoplovstva najvažniji su: Uredba (EU) 2018/1139, Direktiva o sigurnosti mrežnih i informacijskih sustava (*Directive on security of network and information systems* – NIS Directive)/ Direktiva (EU) 2016/1148, Uredba (EZ) br. 300/2008 te Uredba (EU) 2015/1998. Uredba (EU) 2018/1139 relevantna je jer utvrđuje

određena zajednička pravila u području civilnog zrakoplovstva, kao i Uredba (EZ) br. 300/2008, ali i o osnivanju Agencije Europske unije za sigurnost zračnog prometa (*European Union Aviation Safety Agency* - EASA) [7]. EASA je agencija osnovana 2002. godine čija je uloga osigurati sigurnost i zaštitu okoliša u civilnom zrakoplovstvu na području Europe. Smještena je u Kölnu, a države članice su sve države članice EU te Island, Lihtenštajn, Norveška i Švicarska [8].

2.1.1. EU 2015/1998 i EU 2019/1583

Provedbena uredba komisije (EU) 2015/1998 dokument je u kojem su navedene detaljne mjere za provedbu zajedničkih osnovnih standarda iz područja zaštite zračnog prometa. Uredba se sastoji od 12 poglavlja sljedećih naslova [9]:

- Zaštita zračne luke,
- Demarkirane zone u zračnim lukama,
- Zaštita zrakoplova,
- Putnici i ručna prtljaga,
- Predana prtljaga,
- Teret i pošta,
- Kompanijska pošta i kompanijski materijali zračnog prijevoznika,
- Zalihe za opskrbu tijekom leta,
- Zalihe za opskrbu zračnih luka,
- Mjere zaštite tijekom leta,
- Zapošljavanje i osposobljavanje osoblja,
- Zaštitna oprema.

Iako je Uredba komisije (EU) 2015/1998 detaljno obradila područje zaštite zračnog prometa, u njoj su specificirane samo fizičke mjere zaštite tj. mjere zaštite koje napadaču onemogućavaju izravni pristup meti. No, osiguravanje resursa od neovlaštenog fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja ne pokriva sve potencijalne izvore prijetnji. Iz tog razloga jest za sve resurse potrebna i programsko-tehnička zaštita. S ciljem utvrđivanja detaljnih mjera za provedbu zajedničkih osnovnih standarda iz područja zaštite zračnog prometa u pogledu mjera kibernetičke sigurnosti donesena je Uredba komisije (EU) 2019/1583 [10].

Mete kibernetičkih (*cyber*) napada najčešće su kritični informacijski sustavi. Kritični informacijski sustavi su dijelovi kritične infrastrukture koji pružaju osnovne usluge društvu pa su

samim time i okosnica gospodarstva, sigurnosti i zdravlja [11]. Stoga su, prema Uredbi komisije (EU) 2019/1583, nadležna tijela dužna osigurati da svi subjekti definirani u u nacionalnom programu zaštite civilnog zračnog prometa utvrde i štite svoje ključne kritične sustave. Uredba komisije (EU) 2019/1583 također i navodi posebne zahtjeve za provjeru podobnosti i osposobljavanje osoba čije su uloga i odgovornost povezane s kibernetičkim prijetnjama. Prema tome, proširenoj provjeri podobnosti podliježu [10]:

- Osobe zadužene za provedbu zaštitnog pregleda, kontrole pristupa ili drugih zaštitnih kontrola izvan zaštitno ograničenog područja,
- Osobe koje su u mogućnosti bez nadzora ostvariti kontakt sa zračnim teretom i poštom, kompanijskom poštom i materijalima zračnog prijevoznika, zalihama za opskrbu tijekom leta i zalihama za opskrbu zračne luke na koje se primjenjuju zaštitne kontrole,
- Osobe koje su u mogućnosti pristupiti ključnim sustavima informacijske i komunikacijske tehnologije te informacijama korištenim za zaštitu civilnog zrakoplovstva.

2.1.2. Direktiva (EU) 2016/1148/Direktiva NIS

Uočavanje važnosti mrežnih i informacijskih sustava i usluga te uloge koju isti imaju u društvu rezultiralo je donošenjem Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije koja se sastoji od sljedećih poglavlja [12]:

- Opće odredbe,
- Nacionalni okviri za sigurnost mrežnih i informacijskih sustava,
- Suradnja,
- Sigurnost mrežnih i informacijskih sustava operatora ključnih usluga,
- Sigurnost mrežnih i informacijskih sustava pružatelja digitalnih usluga,
- Normizacija i obavješćivanje na dobrovoljnoj osnovi,
- Završne odredbe.

Članak 4. naslova Definicije navodi da se izrazom operator ključne usluge označava javni ili privatni subjekt tipa navedenog u Prilogu 2 [12]. Za sektor prijevoz i podsektor zračni promet, to su:

- Zračni prijevoznici tj. poduzeća za zračni prijevoz koja posjeduju valjanu operativnu licencu ili istovrijedni dokument [13],
- Upravno tijelo zračne luke što znači tijelo kojemu je cilj rukovoditi i upravljati infrastrukturom zračne luke te koordinirati i nadzirati djelatnosti različitih operatora u dotičnoj zračnoj luci [14],
- Zračna luka definirana kao svaka površina namijenjena za slijetanje, polijetanje i manevriranje zrakoplova uključujući i pripadajuće objekte, sredstva i uređaje namijenjene za odvijanje zračnog prometa i pružanje usluga, te objekte, sredstva i uređaje za pomoć u pružanju usluga komercijalnog zračnog prijevoza [14],
- Glavne zračne luke s popisa u 2. odjeljku Priloga II. Uredbi (EU) br. 1315/2013 Europskog parlamenta i Vijeća [12],
- Tijela koja upravljaju pomoćnim objektima u zračnim lukama [12].

Događaj vezan uz zaštitu informacija koji ima potencijal naštetiti imovini ili poslovanju organizacije definira se kao incident vezan uz zaštitu [4]. Prema NIS Direktivi, operateri ključnih usluga dužni su obavijestiti nadležno tijelo ili tim za odgovor na računalne sigurnosne incidente (*Computer Security Incident Response Team* – CSIRT). S ciljem određivanja važnosti učinka nekog incidenta, obavijest mora sadržavati informacije o broju korisnika pogođenih prekidom osnovnih usluga, trajanju incidenta te zemljopisnoj raširenosti u smislu područja na koje bi incident mogao utjecati [12].

2.1.3. Primjena međunarodne regulative na zakone Republike Hrvatske

Zakoni i uredbe Republike Hrvatske vezani uz kibernetičku sigurnost nastali su kao posljedica implementacije europskih direktiva i uredbi. Tako je po uzoru na NIS Direktivu u Hrvatskoj 6. srpnja 2018. godine donesen Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018).

U Prilogu 1. ovog Zakona popisane su ključne usluge s kriterijima i pragovima za utvrđivanje važnosti negativnog učinka incidenta. Podaci za ključne usluge zračnog prometa prikazani su u tablici 1.

Tablica 1. Prikaz kriterija za utvrđivanje negativnog učinka incidenta i pragova za utvrđivanje važnosti negativnog učinka incidenta s obzirom na pojedine ključne usluge

Ključna usluga	Kriteriji za utvrđivanje negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
Zračni prijevoz putnika i tereta	Udio putnika pojedinog zračnog prijevoznika na bilo kojem nacionalnom aerodromu koji ima promet putnika veći od 2 000 000 godišnje (ključni aerodrom)	Zračni prijevoznik koji ima udio veći od 30% na ključnom aerodromu
Upravljanje infrastrukturom zračne luke, uključujući upravljanje pomoćnim objektima zračne luke	Ukupni godišnji promet putnika pojedine zračne luke	Više od 2 000 000 putnika
Kontrola zračnog prometa	Otvorenost područja letnih informacija Zagreb (FIR Zagreb) bez iznimke	-
	Broj operacija na godišnjoj razini	Ukupno 500 000 operacija za FIR Zagreb

Izvor: [15]

Zatim je Vlada Republike Hrvatske 26. srpnja 2018. godine donijela Uredbu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga čime se u hrvatsko zakonodavstvo službeno preuzela NIS Direktiva.

Tom uredbom, u Prilogu 1., popisani su kriteriji za utvđivanje incidenata koji imaju znatan učinak na pružanje ključne usluge u zračnom prometu (navedeni u tablici 2.).

Tablica 2. Kriteriji za utvrđivanje incidenata koji imaju znatan učinak na pružanje ključne usluge

Ključna usluga	Kriteriji	Pragovi
Zračni prijevoz putnika i tereta	Broj putnika pogođenih incidentom na pojedinoj zračnoj luci	20% od uobičajenog prometa
Upravljanje infrastrukturom zračne luke, uključujući upravljanje pomoćnim objektima zračne luke	Broj putnika pogođenih incidentom na pojedinoj zračnoj luci	20% od uobičajenog prometa
Kontrola zračnog prometa	Narušavanje integriteta podataka na ključnim operativnim sustavima	Ugrožen 1 zrakoplov u bilo kojem volumenu kontroliranog zračnog prostora i na manevarskim površinama aerodroma
	Gubitak podataka na ključnim operativnim sustavima	Ugrožen 1 zrakoplov u bilo kojem volumenu kontroliranog zračnog prostora i na manevarskim površinama aerodroma

Izvor: [16]

Sljedeći korak bio je donošenje Smjernica za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga. Prema članku 43. Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, operatori ključnih usluga i davatelji digitalnih usluga dužni su prijaviti incidente koji su nastali kao posljedica izravnog kibernetičkog utjecaja na IT infrastrukturu nadležnom CSIRT-u.

U roku od najviše četiri sata od trenutka otkrivanja incidenta sa znatnim učinkom operator je dužan dostaviti inicijalnu obavijest. Nakon inicijalne obavijesti, a do okončanja incidenta, korisnik će nadležnom CSIRT-u informacije dostavljati putem prijelaznih izvješća. Završno izvješće korisnici su obavezni podnijeti najkasnije 15 dana nakon ponovne uspostave redovnog pružanja usluge [17].

2.1. Praksa

Pri implementaciji zakonske regulative u praksu, pojavili su se određeni mehanizmi primjenjivi za sve sudionike u zračnom prometu kao što su procjena rizika ili osnovnih funkcija i ciljeva koje je naveo američki Nacionalni Institut za standarde i tehnologiju (*National Institute of Standards and Technology* – NIST*)*. Prema NIST-u, nacionalni program zaštite od kibernetičkih prijetnji treba imati pet osnovnih funkcija koje su navedene u tablici 3 [18].

Tablica 3. NIST osnovne funkcije i ciljevi

Osnovna funkcija	Cilj
Identifikacija	Razumijevanje kibernetičkog okruženja
Zaštita	Razvitak i implementacija zaštite
Otkrivanje	Implementacija mjera za brzo otkrivanje događaja vezanog uz kibernetičku zaštitu
Odgovor	Razvitak sposobnosti ograničavanja utjecaja događaja vezanog uz kibernetičku zaštitu
Oporavak	Razvitak sposobnosti ponovne uspostave narušenih sustava

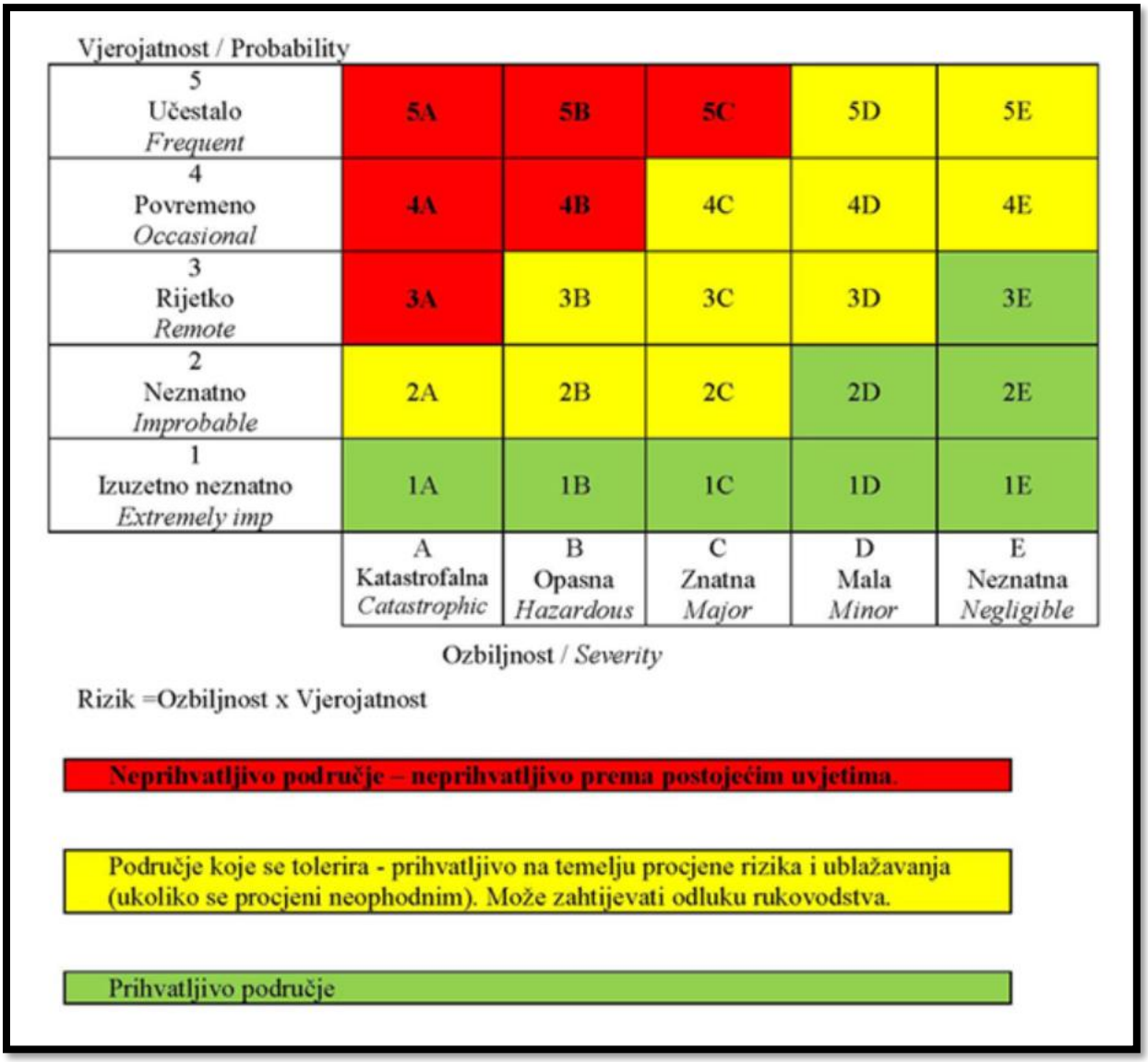
Izvor: [18]

Iako postoje univerzalni mehanizmi za zaštitu od kibernetičkih rizika, pojedini sudionici u zračnom prometu razvijaju vlastite načine zaštite zbog specifičnosti vlastitih kritičnih sustava.

2.2.1. Procjena rizika

Rizik predstavlja procjenu posljedice opasnosti u korelaciji sa vjerojatnošću i ozbiljnošću pri čemu se za referencu uzima najgora moguća situacija. Zbog toga se nakon procjene rizika provodi ublažavanje rizika radi uklanjanja opasnosti ili smanjenja ozbiljnosti ili vjerojatnosti rizika [19]. Prema toj metodi provodi se postupak određivanja, razvitka i primjene detaljnih mjera za zaštitu kritičnih sustava [10]. Upravljanje rizicima definira se kao potencijalno

ostvarenje mogućnosti uz upravljanje neželjenim posljedicama. To je proces u kojem se sustavno primjenjuju politika, procedure i prakse pružatelja usluga kako bi se definirao kontekst, identificirale opasnosti te pratili učinci poduzetih mjera/akcija [19]. Za procjenu rizika tj. opasnosti koristi se matrica rizika prikazana na slici 2.

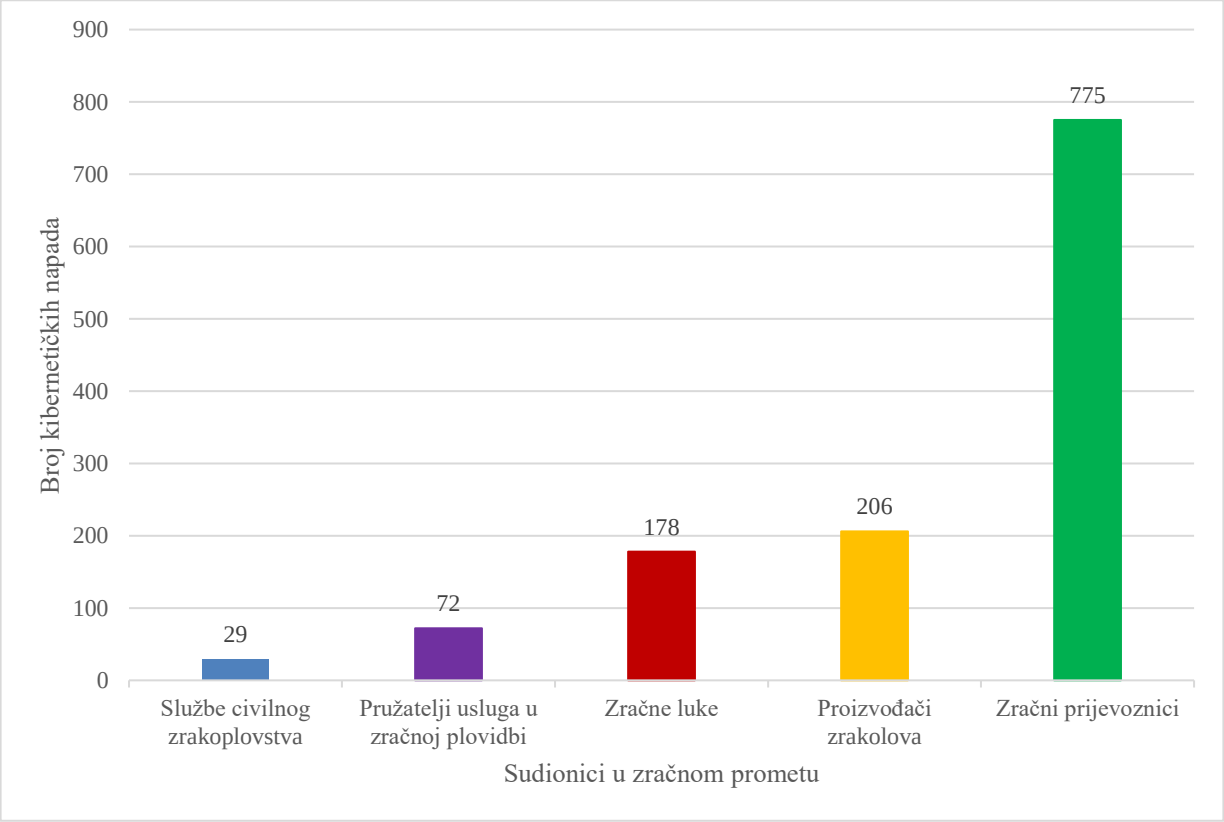


Slika 2. Matrica rizika
Izvor: *[19]*

Svim rizicima se upravlja na način da ih se zadrži na prihvatljivoj razini, i to balansiranjem između vremena, troška i složenosti provođenja mjera. Pri upravljanju rizicima izuzetno su važne i korektivne mjere koje u obzir uzimaju elemente postojeće obrane, ali i potencijalne elemente koji bi aktualnu razinu sigurnosti učinili neodrživom [19].

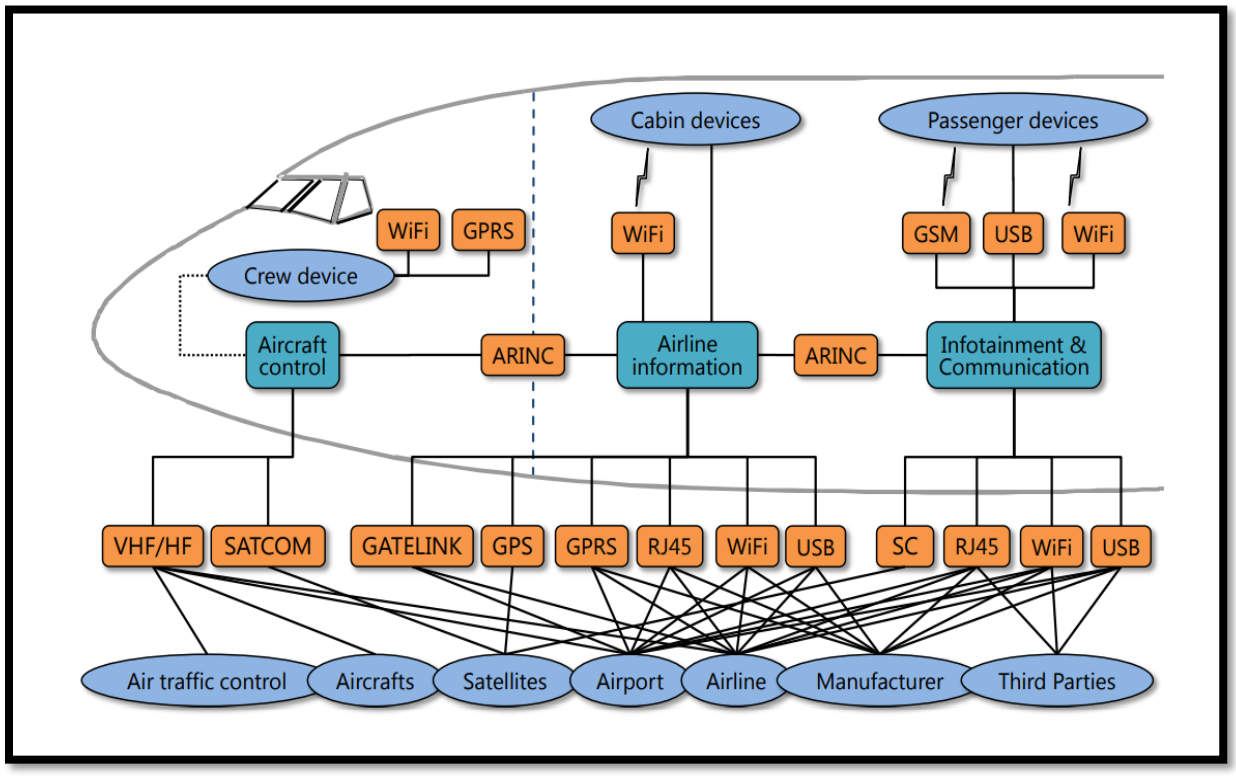
2.2.2. Zaštita pojedinih sudionika u zračnom prometu

Uz putnike, glavni sudionici u zračnom prometu su zračni prijevoznici, zračne luke i pružatelji usluga u zračnoj plovidbi (*Air Navigation Service Provider* – ANSP). Prema istraživanju EUROCONTROL-a, sudionici zračnog prometa koji predstavljaju najciljaniju metu kibernetičkih napada su upravo zračni prijevoznici (graf 1.). Na njih je, u 2020. godini, bilo usmjereno 61% svih detektiranih kibernetičkih napada [20].



Graf 1. Broj detektiranih kibernetičkih napada po pojedinim sudionicima u zračnom prometu u 2020. godini
Izvor: *[20]*

Prema drugom istraživanju, čak 85% izvršnih direktora tvrtki zračnih prijevoznika izražava zabrinutost zbog kibernetičkih rizika kojima su izloženi. Primarni izvor njihovih briga jest zaštita podataka putnika i kompanije, ali i tehnologija koja poboljšava povezanost sustava za operacije letenja sa zemaljskim osobljem i sustavima za pružanje operativnih usluga u zračnom prometu. Iako navedeni sustavi predstavljaju tehnološki napredak, mogu se promatrati i kao prilike za one koji žele naštetiti kritičnim sustavima zračnih prijevoznika. Primjeri za takvu vrstu tehnoloških napredaka su i elektroničke letačke torbe (*Electronic Flight Bags* – EFBs) te sustavi za zabavu tijekom leta (*In-flight Entertainment & Connectivity* – IFEC). EFBs su izrazito popularne kod pilota jer im olakšavaju prijenos stvari, a IFEC sustavi su produktivan marketinški potez jer, prema istraživanju Lufthanse, 83% putnika traži isključivo zračnog prijevoznika koji će im omogućiti Wi-Fi tijekom leta [21] [22]. Osim navedenih dodatnih sadržaja koji stvaraju kibernetičke rizike, u samom zrakoplovu nalazi se znatan broj već postojećih kritičnih sustava koji omogućuju komunikaciju modernih zrakoplova s jedinicama kontrole zračnog prometa, drugim zrakoplovima, zračnim lukama, zračnim prijevoznicima, proizvođačima te trećim stranama koji su prikazani na slici 3 [23].



Slika 3. Velik broj digitalnih komunikacijskih veza modernog zrakoplova
Izvor: *[23]*

Neke od digitalnih komunikacijskih veza, ali i potencijalne ulazne točke za kibernetičke napadače su [23]:

- Radio oprema koja funkcionira na vrlo visokim frekvencijama/visokim frekvencijama,
- Satelitska komunikacija,
- Globalni sustav za određivanje položaja (*Global Positioning System* – GPS),
- Opća radio-usluga za prijenos datoteka (*General Packet Radio Service* – GPRS),
- Globalni sustav za mobilne telekomunikacije (*Global System for Mobile Communications* - GSM), itd.

U slučaju kibernetičkih napada, finacijska šteta zbog potencijalnih tužbi (u slučaju krađe podataka) nije jedino što zabrinjava zračne prijevoznike. Kibernetički proboji utječu i na reputaciju samih prijevoznika što direktno utječe na prodaju karata za njihove letove. No, zračni prijevoznici nisu jedini koji imaju razloga za brigu. Međunarodna kompanija za pružanje zrakoplovnih telekomunikacija (*Société Internationale de Télécommunications Aéronautiques* – SITA) provela je anketu čiji su rezultati pokazali da samo 35% zračnih prijevoznika i 30% zračnih luka smatra da su prikladno zaštićeni od kibernetičkih rizika [24].

Lažne/neovlaštene web-stranice u 2020. godini bile su izvor 56% kibernetičkih napada na zračne luke [20]. Uz tradicionalne dijelove informacijsko-tehnološke infrastrukture kao što su elektronička pošta i internet, potencijalne mete kibernetičkih napada mogu biti [25]:

- Sustavi za kontrolu pristupa i sustavi za otkrivanje upada,
- Radarski sustavi,
- Uređaji za grijanje, ventilaciju i klimatizaciju,
- Bežični i žičani mrežni sustavi,
- Sustavi za upravljanje objektima i pomoćnim sustavima,
- Komunalna infrastruktura, itd.

Metode i sredstva za provedbu kibernetičkih napada na zračne luke mogu biti prijenosne memorijske jedinice (*Universal Serial Bus* – USB), prijenosna računala, bežične pristupne točke, razni USB uređaji (digitalne kamere, MP3 playeri), čovjek koji koristi računalne viruse poput „Trojan“ (napadači koji su prikriveni kao osoblje), optički mediji (CD, DVD), pametni telefoni, elektronička pošta, internetske prevare, itd. Uz to, posljednjih je godina aktualan i trend donošenja vlastitih uređaja (*Bring Your Own Device* – BYOD) zbog kojeg putnici, ali i zaposlenici zračnih luka, donose svoje uređaje (mobitele, tablete, laptope). Ti uređaji mogu, namjerno ili nenamjerno, biti iskorišteni za prikupljanje povjerljivih informacija ili unošenje računalnog virusa [25]. Iako zračne luke pokazuju puno napada u 2020. godini, većina

prijavljenih kibernetičkih napada (80%) nije imala značajan utjecaj na funkcionalnost zračnih luka [20].

Napadi na pružatelje usluga u zračnoj plovidbi činili su manje od 6% sveukupnog broja napada na sudionike u zračnom prometu u 2020. godini. Samo 3% od 72 prijavljena incidenta uzrokovalo je manje poremećaje u radu ANSP-a [20]. Kibernetički napadi na ANSP mogu imati katastrofalne posljedice. Svaki neovlašteni pristup može postati smetnja u redovitoj obradi i praćenju letova. Konkretno, upad u sustav i manipulacija istim lako mogu rezultirati [26]:

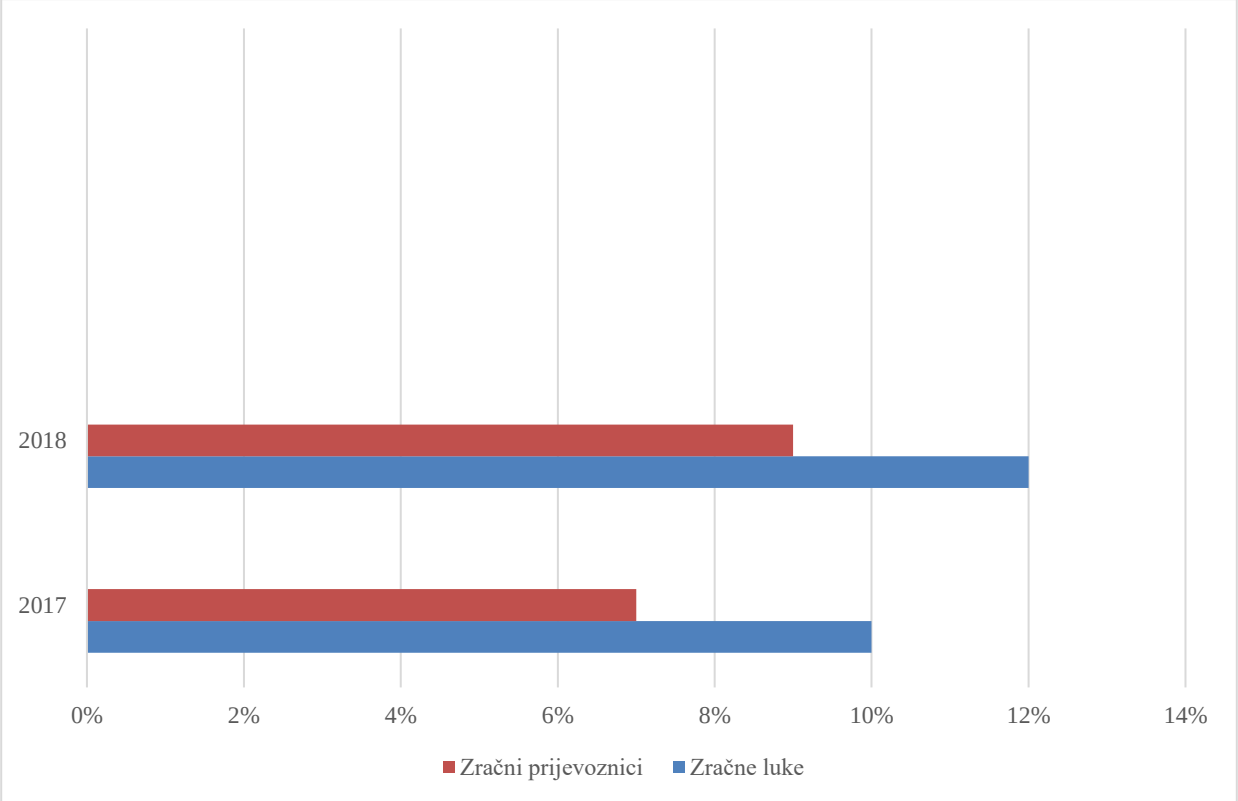
- Otmicom zrakoplova,
- Krađom podataka o zrakoplovu,
- Gubitkom kontrole nad protokom zračnog prometa,
- Nesigurnošću putnika,
- Nesigurnošću zračne luke,
- Krađom drugih povjerljivih podataka.

U praksi, kibernetički napadi na ANSP odvijaju se na način da se komunikacija između zemaljske stanice i zrakoplova (prikazana na slici 4) naruši generiranjem smetnji signala u blizini zemaljske stanice. Zbog toga što aktualne tehnologije ne zahtijevaju provjeru autentičnosti u komunikaciji, moguć je prijenos lažnih informacija ili emisija poruka iz legitimnih izvora koje su modificirane putem snažnih signala [27].

Slika 4. Komunikacija zemaljskih i zračnih stanica sa zrakoplovom
Izvor: *[27]*

Kibernetički napad na pojedinog sudionika zračnog prometa može imati fatalne posljedice za istog, ali i za ostale sudionike zračnog prometa. Iz tog razloga razvijaju se organizacije za razmjenu informaciju o kibernetičkim prijetnjama. Primjer takve organizacije je Centar za dijeljenje i analizu zrakoplovnih informacija (*Aviation Information Sharing and Analysis Center* – A-ISAC), međunarodna neprofitna udruga kojoj je funkcija olakšavanje razmjene slabosti, događaja, obavještajnih podataka o prijetnjama i najboljih praksi za smanjenje operativnih rizika te pružanje sredstava za pouzdanu razmjenu podataka. Aviation ISAC bavi se upravljanjem kibernetičkom zaštitom, mjerenjem kibernetičkih rizika, zaštitom podataka pohranjenih na daljinskom serveru, provođenjem kontrola i upravljanja kod korištenja trećih strana [4], itd.

Posljedica većeg intenziteta kibernetičkih napada su i veća ulaganja pojedinih sudionika zračnog prometa u kibernetički segment zaštite civilnog zrakoplovstva (što je prikazano na grafu 2.).



Graf 2. Postotak IT budžeta uložen u kibernetičku zaštitu
Izvor: *[28]*

3. STATUS KIBERNETIČKE ZAŠTITE CIVILNOG ZRAKOPLOVSTVA

Za definiranje i razumijevanje statusa kibernetičke zaštite civilnog zrakoplovstva potrebno je poznavati osnovne pojmove. Bitno je istaknuti da se neki popisi, opisi i definicije razlikuju od izvora do izvora.

Napadači koji provode kibernetičke prijetnje u djelo različitih su profila, mogu imati različite motive i pristup različitim resursima. Na popisu najčešćih napadača nalaze se [4]:

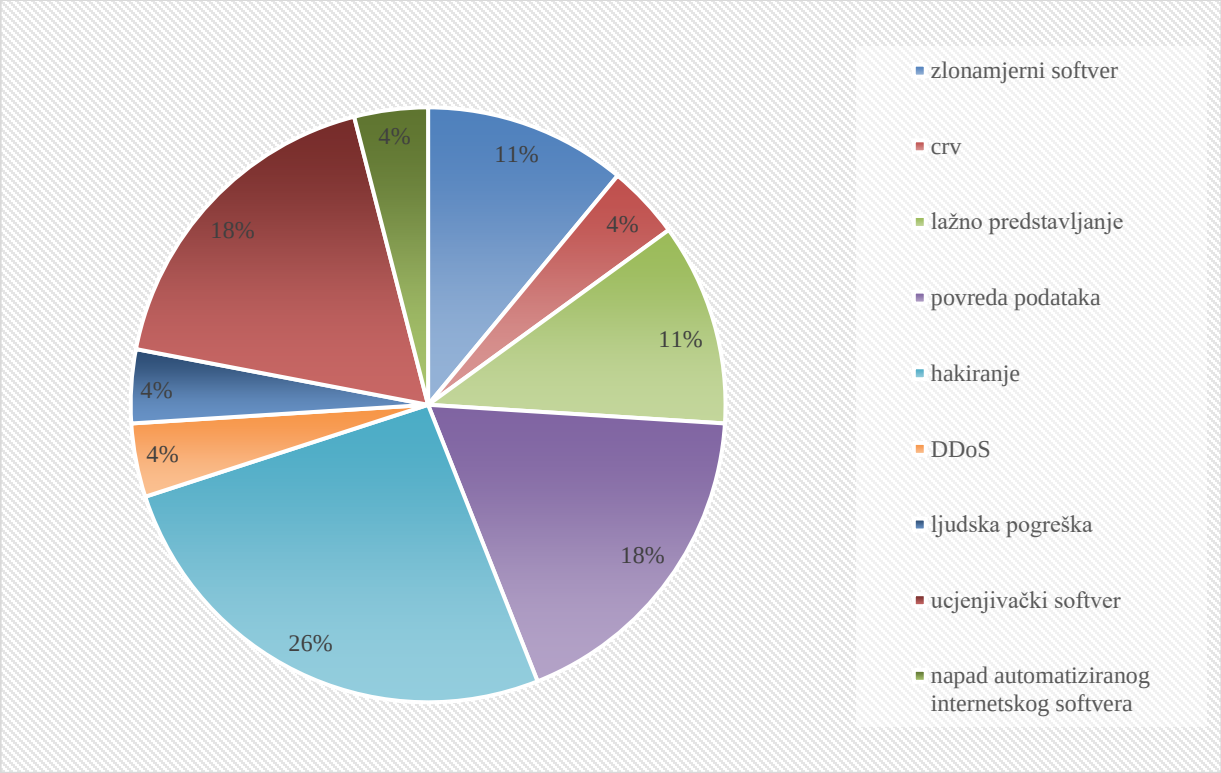
- Vladini hakeri; napadači koji su ujedno i zaposlenici u državnoj vladi, najčešći motiv je ekonomska, politička i/ili vojna prednost,
- Kibernetički kriminalci; najčešći profil napadača, zahtijevaju trenutnu financijsku isplatu,
- Haktivisti; aktivistički hakeri čiji je cilj djelovanja utjecaj na političke ili društvene skupine, privlače medijski fokus i pažnju na sebe, a zatim izvršavaju pritisak na tvrtke, vlade i sl.,
- Teroristi; uzrokuju i šire poremećaj, strah i paniku zbog svojih ideoloških ili političkih uvjerenja,
- Zlonamjerni unutarnji napadači; predstavljaju se kao pouzdani zaposlenici i partneri unutar neke tvrtke, motivi mogu biti osobna dobit, osveta ili novčana nagrada.

Prema težini posljedica i utjecaju koji imaju na odvijanje zračnog prometa, kibernetički napadi mogu se opisati kao lakši, srednji, teški ili kritični napadi [20].

Alati za izvođenje najčešćih kibernetičkih napada su [29]:

- Zlonamjerni softver (*malware*),
- Crv (*worm*),
- Lažno predstavljanje (*phishing*),
- Povreda podataka (*data breach*),
- Hakiranje (*malicious hacking*),
- Distribuirani napadi uskraćivanjem usluga (*Distributed Denial of Service* – DDoS),
- Ljudska pogreška (*human error*),
- Ucjenjivački softver (*ransomware*),
- Napad automatiziranog internetskog softvera (*bot attack*).

Udio pojedinog načina u izvođenju kibernetičkih napada u vremenskom rasponu od 2001. godine do 2021. godine prikazan je na grafu 3.



Graf 3. Udio pojedinog načina izvođenja kibernetičkih napada od 2001. godine do 2021. godine
Izvor: *[29]*

Ovakvo praćenje statusa kibernetičke zaštite po određenim značajkama omogućili su razni izvještaji, ankete i upitnici koji se provode na godišnjim razinama. Najpoznatiji su ENISA Threat Landscape, ISAC Report i EATM-CERT Annual Report on Cyber in Aviation. Zadnji navedeni, godišnji izvještaj o kibernetici u zrakoplovstvu nije dostupan za širu javnost. Naime, kako bi se ojačala sigurnost podataka uveden je tzv. Protokol o semaforu (*Traffic Light Protocol* – TLP) pa se ustupljeni podaci ograničavaju isključivo na ono što je relevantno i nužno. Shodno tome definirane su četiri razine upravljanja informacijama pojašnjene u tablici 4 [26].

Tablica 4. Razine upravljanja informacijama i njihovi opisi

Razina upravljanja informacijama	Opis
Crvena boja (*red*)	Samo za imenovane primatelje, iako se najčešće ovaj tip informacije prenosi verbalno
Boja jantara (*amber*)	Ograničena distribucija, strogo povjerljivo, samo za određene članove unutar zajednice
Zelena boja (*green*)	Informacije u ovoj kategoriji mogu se distribuirati isključivo unutar određene zajednice
Bijela boja (*white*)	Bez ograničenja, podložno standardnim autorskim pravima

Izvor: [26]

3.1. ENISA Threat Landscape 2021.

Agencija Europske unije za kibernetičku sigurnost (*European Union Agency for Cybersecurity* - ENISA) je osnovana 2004. godine u Ateni s ciljem ostvarivanja visoke razine kibernetičke sigurnosti u Europi. Uz ostale aktivnosti, ENISA objavljuje brojne publikacije kao što su mišljenja, informativne bilješke, poslovni dokumenti te službeni izvještaji vezani uz kibernetičku sigurnost [30]. Jedan takav izvještaj jest i ENISA pregled prijetnji za 2021. godinu koji se sastoji od sljedećih 10 poglavlja [31]:

- Općenit pregled prijetnji,
- Trendovi napadača,
- Ucjenjivački softver,
- Zlonamjerni softver,
- Otmica radi rudarenja kripto valuta,
- Prijetnje povezane s elektroničkom poštom,
- Prijetnje podacima,
- Prijetnje dostupnosti i integritetu,
- Dezinformacije,
- Nenamjerne prijetnje.

U prvom poglavlju ENISA pregleda prijetnji (*ENISA Threat Landscape* - ETL) uz popis najopasnijih prijetnji (ucjenjivački softveri, zlonamjerni softveri, otmice radi rudarenja kriptovalutama, prijetnje povezane s elektroničkom poštom, prijetnje podacima, prijetnje

dostupnosti i integritetu, dezinformacije i nenamjerne prijetnje), nalaze se i ključni trendovi, klasifikacija blizine prijetnji, objašnjenje metodologije ENISA-e te opis strukture samoga izvješća. Neki od ključnih trendova su [31]:

- COVID-19 dodatno je potaknuo kibernetičku špijunažu, a rad na daljinu stvorio je nove prilike za kibernetičke kriminalce,
- Vladine organizacije su na nacionalnoj i međunarodnoj razini uložile dodatne napore kako bi onemogućile napadače pod pokroviteljstvom stranih država te poduzele pravne mjere protiv istih,
- Najčešći način isplaćivanja kibernetičkih kriminalaca ostaje kripto valuta,
- Dezinformacije su srž kibernetičkih kriminalnih aktivnosti koje su sve učestalije,
- Zabilježen je porast nenamjernih prijetnji prema računarstvu u „računarstvu u oblaku" (*cloud computing*).

ETL iznosi da je blizina kibernetičkih prijetnji s obzirom na granice EU bitan parametar prijetnji jer se na taj način može lakše analizirati te procjenjivati njihova važnost. Klasifikacija blizine kibernetičkih prijetnji u četiri kategorije prikazana je u tablici 5.

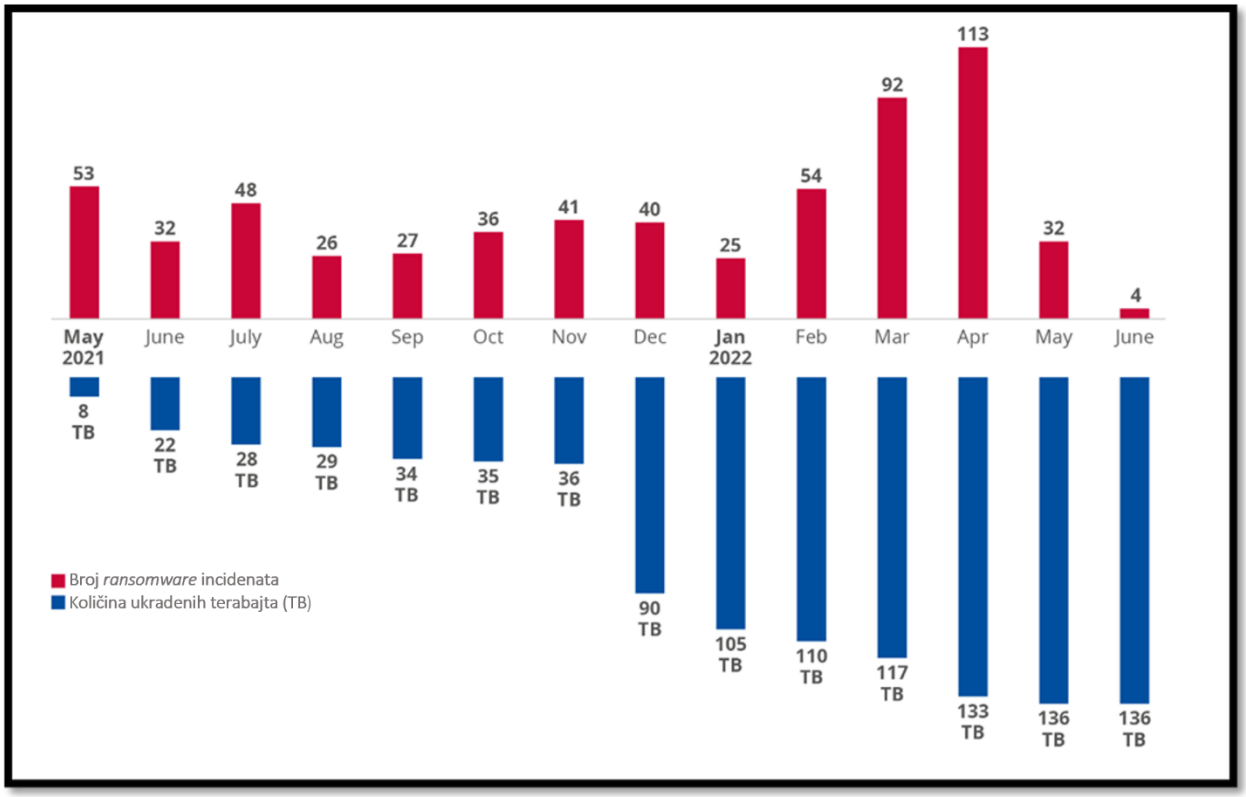
Tablica 5. Klasifikacija blizine kibernetičkih prijetnji

Blizina	Opis
Bliske	Zahvaćeni mreže i sustavi kontrolirani unutar granica EU, pogođena populacija unutar EU
Srednje	Zahvaćeni mreže i sustavi koji se smatraju vitalnim za jedinstveno digitalno tržište EU-a, pogođena populacija u područjima koja su blizu granica EU
Udaljene	Zahvaćeni mreže i sustavi koji bi, pod krivim utjecajem, mogli imati teške posljedice za jedinstveno digitalnte tržište EU-a, pogođena populacija u područjima koja su daleko od granica EU
Globalne	Zahvaćena sva prethodno navedena područja

Izvor: *[31]*

U drugom poglavlju istražuju se trendovi vezani uz napadače pod pokroviteljstvom države (*state-sponsored actors*), kibernetičke kriminalce (*cybercrime actors*), hakeri koji „iznajmljuju“ svoje vještine (*hacker-for-hire actors*) i haktivisti (*hacktivists*) [31].

Treće poglavlje je izvještaj o ucjenjivačkim softverima (*ransomware*). *Ransomware* je vrsta štetnog softvera koji onemogućuje korisniku pristup njegovim vlastitim računalnim resursima sve dok žrtva ne plati otkupninu. Prema izvještaju EUROCONTROL-a, barem jednom tjedno neki od sudionika zračnog prometa bude meta ucjenjivačkih softvera [20]. Osim što su napadi ucjenjivačkim softverima izuzetno česti, zamijećen je i porast količine ukradenih podataka što je i prikazano u grafu 4 za razdoblje od svibnja 2021. godine do lipnja 2022. godine [32].



Graf 4. Broj *ransomware* incidenata i količina podataka koji su ukradeni u razdoblju od svibnja 2021. godine do lipnja 2022. godine
Izvor: *[32]*

Četvrto poglavlje odnosi se na zlonamjerne softvere (*malware*). *Malware* je širok pojam koji obuhvaća softvere, ugrađene programe i kodove namijenjene za izvršenje neovlaštene obrade podataka koja rezultira ugrožavanjem povjerljivosti, cjelovitosti ili dostupnosti sustava. Broj napada zlonamjernih sustava značajno se smanjio. Pad je za 2020. godinu u odnosu na 2019. godinu iznosio oko 43% za područje Sjeverne Amerike i Europe, a 53% za Aziju. Taj trend se nastavio i u 2021. godini kada je sveukupan pad intenziteta *malware*-a iznosio 22% [31].

Kibernetički napadi kojima je cilj otuđivanje kripto valuta tema su petog poglavlja. *Cryptojacking* je vrsta kibernetičkog zločina pri kojem napadač potajno koristi žrtvine resurse kako bi generirao kripto valutu. To se najčešće događa kada žrtva instalira program u kojem su skriveni zlonamjerni kodovi koji omogućuju napadaču pristup žrtvinom računalu. *Cryptojacking* je rastući trend što je posljedica promjenjivosti tržišta kripto valuta [31].

Šesto poglavlje odnosi se na prijetnje povezane s elektroničkom poštom koje su kontinuirano na vrhu popisa prijetnji ETL-a kroz godine. Ove vrste napada nisu posljedica tehničkih manjkavosti informatičkih sustava, već rezultat ljudske nesmotrenosti i navika.

Najpoznatije podvrste ovih prijetnji su: mrežna krađa identiteta (*phishing*), *spear-phishing* (naziv za napade koji ciljaju specifične organizacije ili pojedince), *whaling* (*spear-phishing* napadi koji čije su mete visokoprofilne žrtve poput izvršnih direktora ili političara), *smishing* (izraz koji je nastao spajanjem riječi *SMS* i *phishing*) gdje se osobni podaci žrtava prikupljaju putem poruka, te neželjena pošta (*spam*). U 2021. godini najčešća prijetnja vezana uz elektroničku poštu bio je *spam* za koji je mamac bila tematika virus COVID-19 [31].

Naslov sedmog poglavlja je prijetnje podacima. Kod prijetnji podacima, meta su izvori podataka kojima napadači pokušavaju neovlašteno pristupiti, objaviti te podatke ili na temelju njih širiti dezinformacije. Drugi nazivi su curenje podataka ili povreda podataka. Prema ETL-u, ove prijetnje također spadaju u grupu najčešćih kibernetičkih prijetnji [31].

Dostupnost i integritet, tema osmog poglavlja, mete su brojnih napada i prijetnji od kojih su najpoznatiji DDoS i napadi bazirani na *web* sustavima (*web-based attacks*). Distribuirani napadi uskraćivanjem usluga rezultiraju nemogućnošću korisnika da pristupi važnim informacijama, uslugama ili drugim resursima, čime je direktno napadnuta dostupnost nekog sustava. S druge strane, napadi bazirani na *web* sustavima ugrožavaju i integritet i dostupnost sustava. [31]

Naslov devetog poglavlja su dezinformacije. Dezinformacije su netočne ili obmanjujuće informacije na kojima se bazira *phishing*. Kombinacija dezinformacija i *phishing*-a klasificira se kao hibridna prijetnja [31].

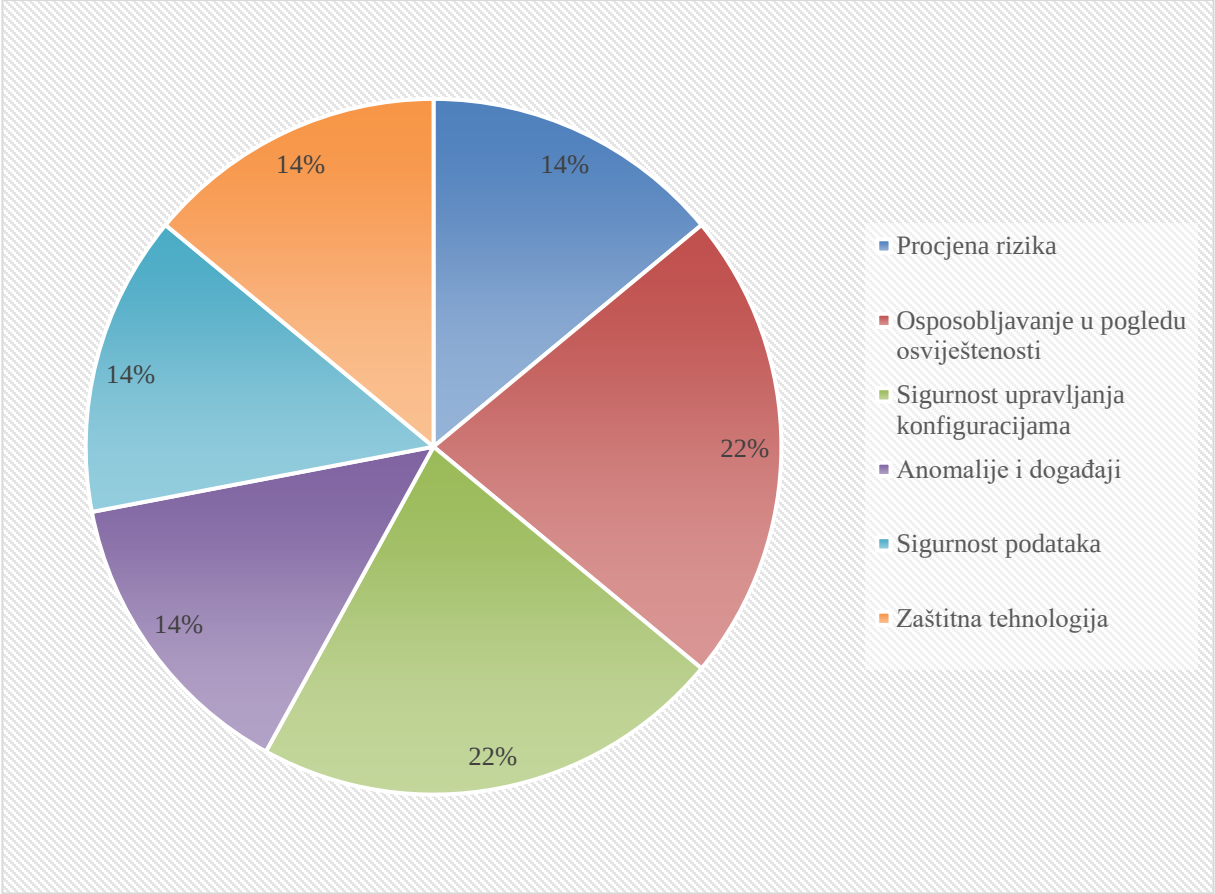
U desetom poglavlju opisane su nenamjerne prijetnje koje se najčešće događaju zbog ljudske pogreške ili pogrešne konfiguracije sustava. Iako nisu ciljane tj. namjerne, ove prijetnje također stvaraju sigurnosnu ugrozu [31].

3.2. Aviation ISAC 2022. Cyber Risk Survey

Petu godinu za redom A-ISAC provodi godišnje istraživanje o kibernetičkim rizicima. Rezultati služe kao naputak, svojevrsna smjernica o područjima kibernetičke sigurnosti u zrakoplovstvu koje je potrebno kontinuirano ojačavati. Rezultati istraživanja grupiraju se u tri segmenta; rezultate vezane uz zračne prijevoznike, rezultate vezane uz zračne luke i rezultate vezane uz proizvođače originalne opreme (*Original Equipment Manufacturers* – OEM). U 2022. godini, pet glavnih inicijativa za smanjenje kibernetičkih rizika su [33]:

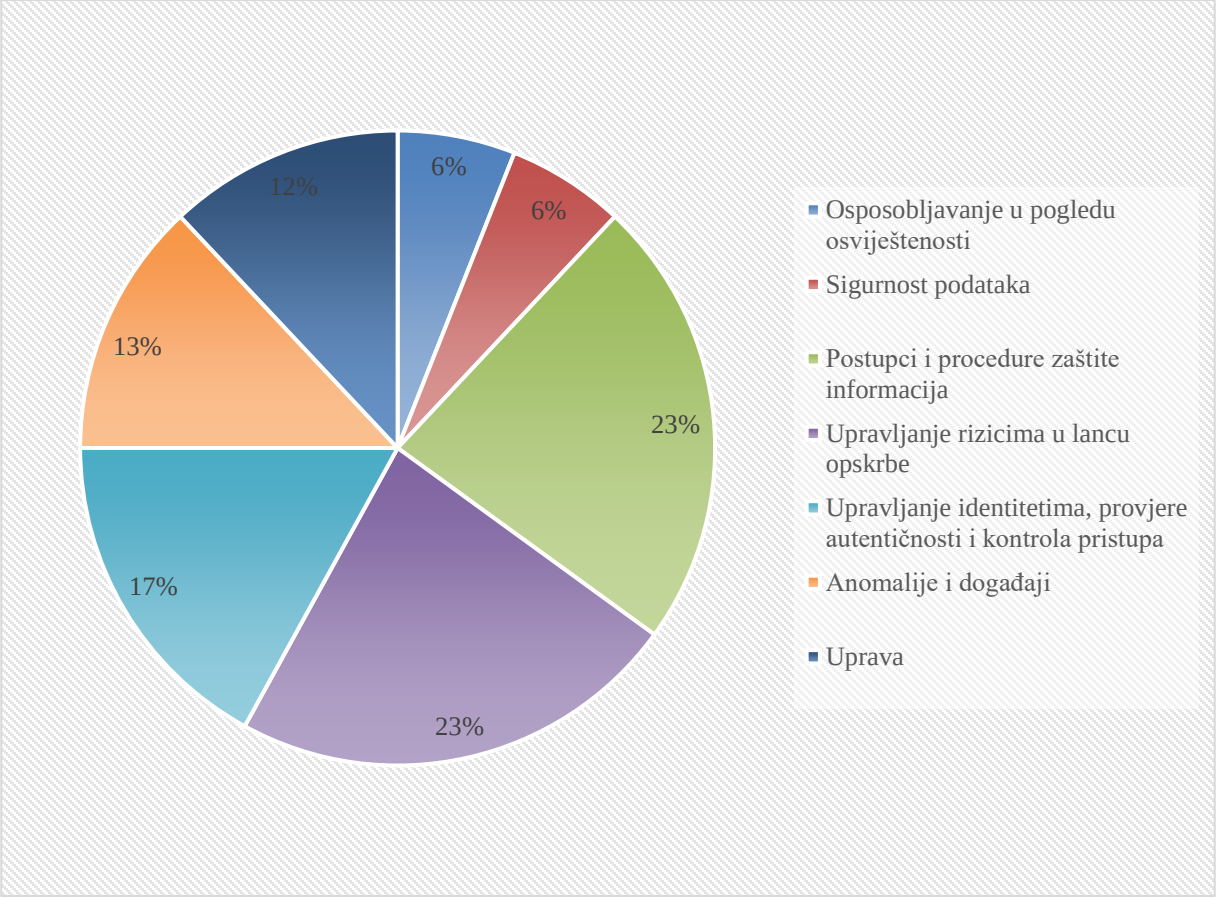
- Upravljanje identitetima (*Identity Management* – IDM), provjere autentičnosti (*Authentication*) i kontrola pristupa (*Access Control*),
- Procesi i postupci zaštite informacija (*Information Protection Processes and Procedures* – IPPP),
- Upravljanje rizicima u lancu opskrbe (*Supply Chain Risk Management*),
- Sigurnost podataka (*Data Security*),
- Anomalije i događaji (*Anomalies and Events*).

2022. godina za zračne luke predstavlja period u kojem je fokus na podizanju svijesti i osposobljavanju osoblja. Uvodi se inicijativa za tzv. Centar za operativnu sigurnost (Security Operations Center – SOC) preko kojega se kontinuiranim nadgledanjem prate sredstva i lakše uočavaju anomalije. Zastupljenost pojedinih inicijativa kibernetičke sigurnosti za zračne luke prikazane je na grafu 5 [33].



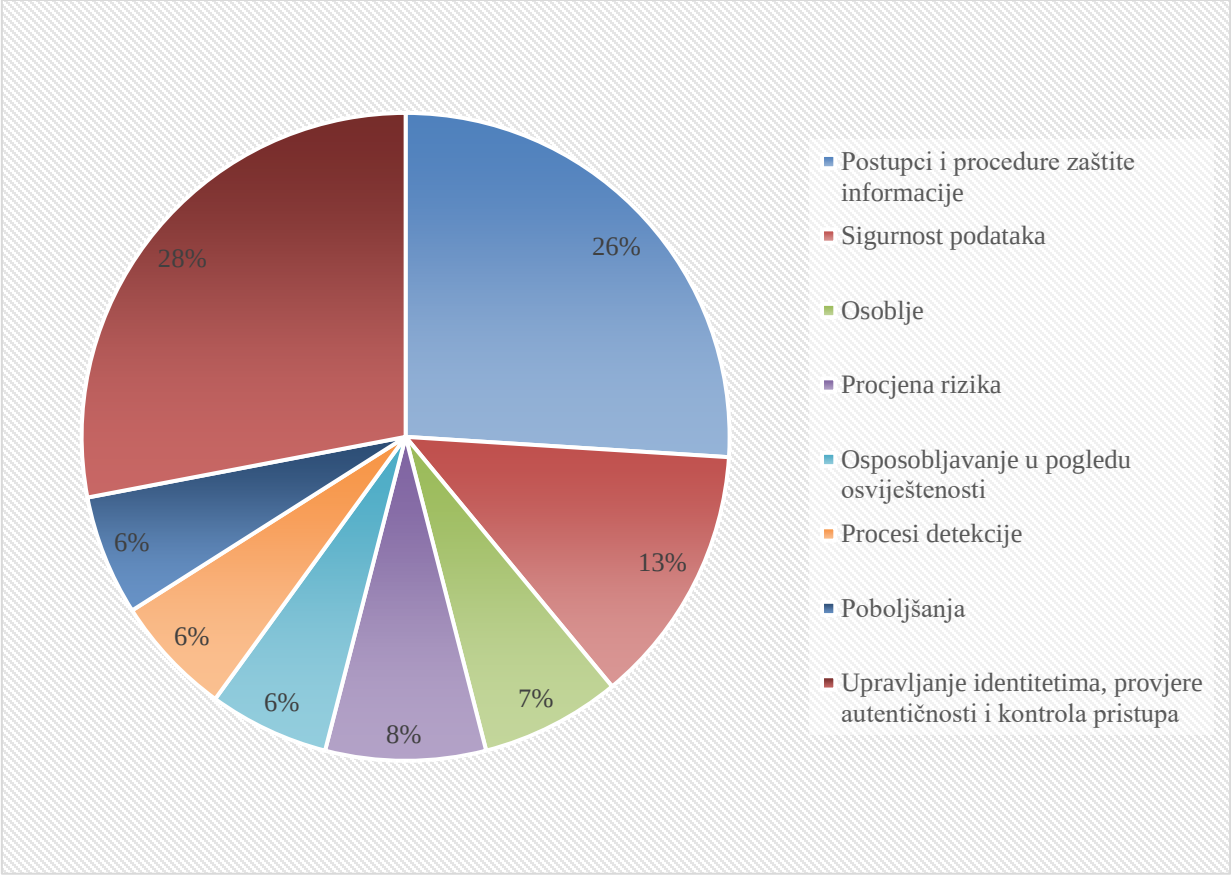
Graf 5. Zastupljenost pojedinih inicijativa kibernetičke sigurnosti za zračne luke
Izvor: *[33]*

Proizvođači originalne opreme usmjereni su na upravljanje identitetima, provjere autentičnosti i kontrolu pristupa, dok procesi i postupci zaštite informacija te upravljanje rizicima u lancu opskrbe za njih predstavljaju nove i rastuće trendove. Detaljna zastupljenost pojedinih inicijativa prikazana je na grafu 6 [33].



Graf 6. Zastupljenost pojedinih inicijativa kibernetičke sigurnosti za proizvođače originalne opreme
Izvor: *[33]*

Upravljanje identitetima, provjere autentičnosti i kontrola pristupa primarni su fokus i kod zračnih prijevoznika. Procesi i postupci zaštite informacija te sigurnost podataka dvije su kategorije koje primaju znatno više sredstava u odnosu na ostale kategorije. Zastupljenost glavnih inicijativa kibernetičke sigurnosti za zračne prijevoznike prikazana je u grafu 7 [33].



Graf 7. Zastupljenost pojedinih inicijativa kibernetičke sigurnosti za zračne prijevoznike
Izvor: *[33]*

3.3. Najpoznatiji kibernetički napadi u zrakoplovstvu

Status kibernetičke zaštite u zrakoplovstvu tj. postojanost i funkcionalnost iste također odlično dočaravaju i napadi koji su se već zbili jer omogućuju praćenje napretka zaštite. U nastavku se nalazi popis pet najznačajnijih kibernetičkih napada u povijesti zrakoplovstva navedenih po težini napada, financijskim posljedicama i/ili količini ukradenih podataka [24]:

- Cathay Pacific Airways
  Incident je po broju ukradenih podataka najpoznatiji u zrakoplovnoj povijesti. U ožujku 2018. godine, IT tim detektirao je sumnjivu aktivnost koja se kasnije pokazala kao neovlašten pristup sustavu putem servera povezanog s internetom. Ukradeni podaci uključivali su podatke s putovnica, datume rođenja, brojeve

telefona, informacije o kreditnim karticama i sl. Ovim probojem otuđeni su podaci od rekordnih 9.4 milijuna putnika.

- EasyJet

  Navedeni britanski niskotarifni prijevoznik u svibnju 2020. godine otkrio je javnosti da su u siječnju iste godine bili žrtvom veoma sofisticiranog kibernetičkog napada u kojem su se hakeri domogli e-mail adresa, informacija o putovanju i informacija o kreditnim karticama devet milijuna EasyJet-ovih putnika. Kao posljedica "curenja" informacija, ali i zataškavanja od strane prijevoznika u trajanju od četiri mjeseca, EasyJet se morao suočiti s 10 000 klijenata koji su tužili kompaniju, a vrijednost tužbe iznosila 18 milijardi britanskih funti.

- SITA

  SITA, kompanija koja pruža zrakoplovne informacije, u travnju 2021. godine potvrdila je tešku povredu svojih podatkovnih baza kao posljedicu kibernetičkih napada fokusiranih na sustav usluga za putnike (*Passenger Service System* - PSS). Pri tome napadu otkriveni su brojevi kartica programa, statusi i imena više od dva milijuna putnika. No, prema navodima glasnogovornika SITA-e, od napada su sačuvane e-mail adrese i lozinke putnika.

- British Airways

  Iz British Airways-a priznali su otuđivanje podataka 429 612 putnika u razdoblju od 15 dana tijekom 2018. godine. Osim što su otuđeni podaci putnika (imena, adrese, podaci s kreditnih kartica), istraga je pokazala propuste od strane prijevoznika koja ih je prokazala kao krivca za nedovoljnu zaštitu podataka putnika te su kažnjeni s 20 milijuna britanskih funti.

- Air Canada

  U kolovozu 2018. godine, hakeri su napali mobilnu aplikaciju Air Canade otuđivši podatke preko 20 000 korisnika, a u aplikaciji su bili upisani brojevi telefona, e-mail adrese i imena putnika. Aplikacija je zbog proboja zaključana te niti jedan od 1.7 milijuna korisnika nisu bili u mogućnosti pristupiti svojim računima dok nisu promijenili lozinku.

4. PREVENTIVNE MJERE KIBERNETIČKE ZAŠTITE CIVILNOG ZRAKOPLOVSTVA

Međunarodna organizacija za normizaciju (*International Organization for Standardization* – ISO) je međunarodno tijelo sa svrhom donošenja normi od kojih su najpoznatiji standardi vezani uz upravljanje kvalitetom (*ISO 9000 family*), upravljanje zaštitom okoliša (*ISO 14000 family*) te upravljanje sigurnošću informacija (*ISO/IEC 27000*) [34]. *ISO/IEC 27001* je set normi za razne sektore sigurnosti, u čijoj je izradi sudjelovalo i Međunarodno elektrotehničko povjerenstvo (*International Electrotechnical Commission* – IEC), uključujući zahtjeve za Sustav upravljanja sigurnošću informacija (*Information Security Management System* – ISMS) [35]. Jedan od glavnih procesa temeljnih za implementaciju ISMS-a u organizaciju je skeniranje ranjivosti preko kojeg je moguće testirati, identificirati i analizirati potencijalne sigurnosne probleme mreže. Čak 73% zrakoplovnih organizacija ima implementiran ISMS [20].

Uz glavni dio u kojem su navedeni zahtjevi vezani uz razumijevanje organizacije, kompetetnost, komunikaciju i sam ISMS, u *ISO/IEC 27001* nalazi se i Aneks A podijeljen u 13 poglavlja. Za preventivne mjere kibernetičke zaštite ističe se dio A.6 Organizacija informacijske sigurnosti (*Organisation of information security*) čiji su najvažniji podnaslovi [36]:

- A.6.1.1 Uloge informacijske sigurnosti i odgovornosti (*Information Security Roles & Responsibilities*)
  Sve odgovornosti vezane uz informacijsku sigurnost moraju biti točno definirane, označene kao opće i/ili specifične i dodijeljene;
- A.6.1.2 Podjela dužnosti (*Segregation of Duties*)
  Oprečne dužnosti i područja odgovornosti moraju biti podijeljeni kako bi se smanjila mogućnost neovlaštene ili nenamjerne upotrebe sredstava organizacije;
- A.6.1.3 Kontakt s vlastima (*Contact with Authorities*)
  Prikladan kontakt mora biti održavan s nadležnim tijelima pri čemu je nužno razmotriti kako će se kontakt ostvarivati, tko će ga i pod kojim okolnostima ostvarivati te koja je priroda informacija koje će biti podijeljene;
- A.6.1.4 Kontakti s posebnim interesnim skupinama (*Contact with Special Interest Groups*)
  Također je potrebno održavati prikladan kontakt s posebnim interesnim skupinama, a prije toga je nužno razumjeti osobine i namjeru tih skupina;
- A.6.1.5 Informacijska sigurnost u upravljanju projektima (*Information Security in Project Management*)

Informacijska sigurnost mora biti ukorijenjena u strukturi same organizacije, a time i u upravljanju projektima. Preporuka je korištenje obrazaca koji će uključivati kontrolnu listu u okviru svakog projekta, a u kojoj će biti naznačeno da je informacijska sigurnost uzeta u obzir;

- A.6.2.1 Pravilnici o mobilnim uređajima (*Mobile Device Policy*)
  Pravilnik i pripadajuće mjere zaštite moraju biti implementirane kako bi se smanjio rizik koji donosi korištenje mobitela, laptopa, tableta, itd. Predlaže se implementacija strategije temeljite obrane (*Defence in Depth*) čiji su najbitniji segmenti edukacija, trening i podizanje svijesti o korištenju mobilnih uređaja i posljedicama koje isti mogu uzrokovati;
- A.6.2.2 Rad na daljinu (*Teleworking*)
  Također je bitno implementirati i pravilnik te pripadajuće preventivne mjere kako bi se zaštitile informacije kojima se pristupa i koje se obrađuje na daljinu. Za osoblje koje obavlja rad na daljinu, nužni su edukacija, trening i podizanje svijesti.

4.1. Uloge informacijske sigurnosti i odgovornosti

Sve odgovornosti za informacijsku zaštitu moraju biti definirane i dodijeljene. Odgovornosti za informacijsku zaštitu mogu biti opće (npr. zaštita informacija) i/ili specifične (npr. odgovornost za davanje određene dozvole).

Prilikom utvrđivanja odgovornosti treba uzeti u obzir vlasništvo nad informacijskom imovinom ili skupinom imovine. Neki primjeri poslovnih uloga koje imaju određenu važnost za informacijsku zaštitu uključuju voditelje odjela, vlasnike poslovnih procesa; voditelje objekata; HR rukovoditelje i interne auditore.

Auditor nastoji steći sigurnost da je organizacija jasno dala do znanja tko je za što odgovoran na odgovarajući i razmjeran način u skladu s veličinom i prirodom organizacije. Za manje organizacije općenito je nerealno imati uloge s punim radnim vremenom povezane s tim ulogama i odgovornostima.

Kao takvo, važno je pojašnjavanje specifičnih odgovornosti za informacijsku zaštitu unutar postojećih radnih uloga, npr. direktor operacija ili izvršni direktor također može biti ekvivalent glavnom službeniku za informacijsku zaštitu, s glavnom odgovornošću za cijeli ISMS. Tehnički direktor može posjedovati svu informacijsku imovinu povezanu s tehnologijom, itd.

4.2. Podjela dužnosti

Sukobljene dužnosti i područja odgovornosti moraju biti razdvojeni kako bi se smanjile mogućnosti neovlaštene ili nenamjerne izmjene ili zlouporabe bilo koje imovine organizacije.

Organizacija se mora zapitati je li razdvajanje dužnosti razmotreno i provedeno tamo gdje je to prikladno. Manje organizacije mogu imati problema s tim, ali to načelo treba primijeniti što je više moguće i dobro upravljanje i kontrole postaviti za informacijsku imovinu većeg rizika/više vrijednosti, obuhvaćenu kao dio procjene i tretmana rizika.

4.3. Kontakt s vlastima

Moraju se održavati odgovarajući kontakti s nadležnim tijelima. Prilikom prilagodbe ove kontrole treba imati na umu i zakonske odgovornosti za kontaktiranje tijela kao što su policija, ured povjerenika za informiranje ili druga regulatorna tijela, npr. oko GDPR-a. Treba razmotriti kako će se taj kontakt uspostaviti, tko će ga izvršiti, pod kojim okolnostima i prirodu informacija koje treba dati.

4.4. Kontakti s posebnim interesnim skupinama

Također se moraju održavati odgovarajući kontakti s posebnim interesnim skupinama ili drugim specijaliziranim i profesionalnim udrugama. Kada se ova kontrola prilagođava specifičnim potrebama, treba računati da se članstvo u profesionalnim tijelima, industrijskim organizacijama, forumima i grupama za raspravu, ubraja u ovu kontrolu. Važno je razumjeti prirodu svake od ovih grupa i za koju su svrhu osnovane (npr. postoji li komercijalna svrha iza toga).

4.5. Informacijska sigurnost u upravljanju projektima

U upravljanju projektima treba se također osvrnuti i na informacijsku zaštitu, bez obzira na vrstu projekta. Informacijska zaštita treba biti ukorijenjena u tkivo organizacije, a upravljanje

projektima ključno je područje za to. Preporučuje se korištenje okvira predložaka za projekte koji uključuju jednostavan popis za provjeru koji se može ponavljati kako bi se pokazalo da se razmatra zaštita informacija.

Auditor nastoji utvrditi imaju li svi uključeni u projekte zadatak razmotriti informacijsku zaštitu u svim fazama projekta, odnosno to bi trebalo biti obuhvaćeno kao dio obrazovanja i podizanja svijesti u skladu sa općim načelima zaštite.

Organizacije s povezanim obvezama za osobne podatke trebaju razmotriti zaštitu po dizajnu zajedno s procjenom učinka na zaštitu podataka (*Data Protection Impact Assessments* – DPIA) i sličnim procesima kako bi dokazali usklađenost s Općom uredbom o zaštiti podataka (*General Data Protection Regulation* – GDPR) i Zakonom o zaštiti podataka iz 2018 (*Data Protection Act 2018*).

4.6. Pravilnici o mobilnim uređajima

Potrebno je usvojiti politiku i prateće sigurnosne mjere za upravljanje rizicima koji nastaju korištenjem mobilnih telefona i drugih mobilnih uređaja kao što su prijenosna računala, tableti, itd. Kako mobilni uređaji postaju sve „pametniji“, ovo područje politike postaje mnogo značajnije od tradicionalne upotrebe mobilnih uređaja. Korištenje mobilnih uređaja i rad na daljinu ujedno su izvrsna prilika za fleksibilan rad, no i potencijalna sigurnosna ranjivost u smislu zaštite informacija.

BYOD (*Bring Your Own Device*) također treba razmotriti. Iako postoje goleme prednosti omogućavanja osoblju da koristi svoje vlastite uređaje, bez odgovarajuće kontrole, prijetnje također mogu biti značajne.

Organizacija mora biti zaštićena tako da kada se koriste mobilni uređaji ili osoblje koje radi izvan lokacije, njezini podaci i podaci klijenata i drugih zainteresiranih strana ostanu zaštićeni i pod njezinom kontrolom. To postaje sve teže s potrošačkom pohranom u oblaku, automatiziranom sigurnosnom kopijom i uređajima u osobnom vlasništvu koje dijele članovi obitelji.

Organizacija treba razmotriti provedbu strategije „dubinske obrane“ (*Defence in Depth*) s kombinacijom komplementarnih fizičkih, tehničkih i političkih kontrola. Jedan od najvažnijih aspekata je obrazovanje, obuka i svijest o korištenju mobilnih uređaja na javnim mjestima, te

izbjegavanju rizika „besplatne“ internetske veze koja bi mogla brzo kompromitirati informacije ili privući nepozvane promatrače, npr. koji gledaju u zaslon tijekom putovanja.

Auditor treba utvrditi postoje li uspostavljene jasne politike i kontrole koje osiguravaju da informacije ostaju sigurne kada se poslovi obavljaju izvan fizičkih lokacija organizacije. Politike bi trebale pokrivati sljedeća područja:

- registraciju i upravljanje,
- fizičku zaštitu,
- ograničenja u pogledu toga koji se softver može instalirati, koje se usluge i aplikacije mogu dodavati i pristupati, korištenje ovlaštenih i neovlaštenih programera,
- operativna ažuriranja uređaja i aplikacija,
- dostupnost klasifikacije informacija i sva druga ograničenja pristupa imovini (npr. nema pristupa imovini kritične infrastrukture),
- kriptografija, *malware* i antivirusna očekivanja,
- zahtjeve za prijavu, daljinsko onemogućavanje, brisanje, zaključavanje i mogućnost „pronađi moj uređaj“,
- sigurnosna kopija i pohrana,
- obiteljski i drugi uvjeti korisničkog pristupa (ako je BYOD), npr. razdvajanje računa,
- korištenje na javnim mjestima,
- povezivost i pouzdane mreže.

4.7. Rad na daljinu

Politika i prateće sigurnosne mjere također se moraju primijeniti kako bi se zaštitile informacije kojima se pristupa, koje se obrađuju ili pohranjuju na mjestima za daljinski rad. Rad na daljinu odnosi se na rad od kuće i drugi rad izvan mjesta rada, kao što je rad kod dobavljača ili klijenata. Za osoblje koje radi na daljinu, obrazovanje, obuka i svijest o potencijalnim rizicima su ključni.

Auditor treba utvrditi da li postoje odluke koje se odnose na upotrebu mobilnih uređaja za rad na daljinu te sigurnosne mjere temeljene na odgovarajućoj procjeni rizika, balansirajući potrebu za fleksibilnim radom s potencijalnim prijetnjama i ranjivostima koje bi takav način mogao dovesti.

5. INOVATIVNI SUSTAVI UPRAVLJANJA KIBERNETIČKOM ZAŠTITOM U ZRAKOPLOVSTVU

Moderni zračni promet s tehnološkog aspekta definiraju kontinuirani tehnološki napreci. No, tehnološki napreci direktno povećavaju ranjivost pojedinih sustava. Kako bi kibernetička zaštita u zrakoplovstvu bila otporna, brza i pouzdana, potrebno je ulagati u sofsticirane projekte koji će moći detektirati potencijalne sigurnosne proboje, zaštititi sustave i odgovoriti na rastući broj kibernetičkih napada [37].

Inovativni sustavi čiji je cilj upravljanje kibernetičkom zaštitom u zrakoplovstvu uglavnom obuhvaćaju sljedeća područja [37]:

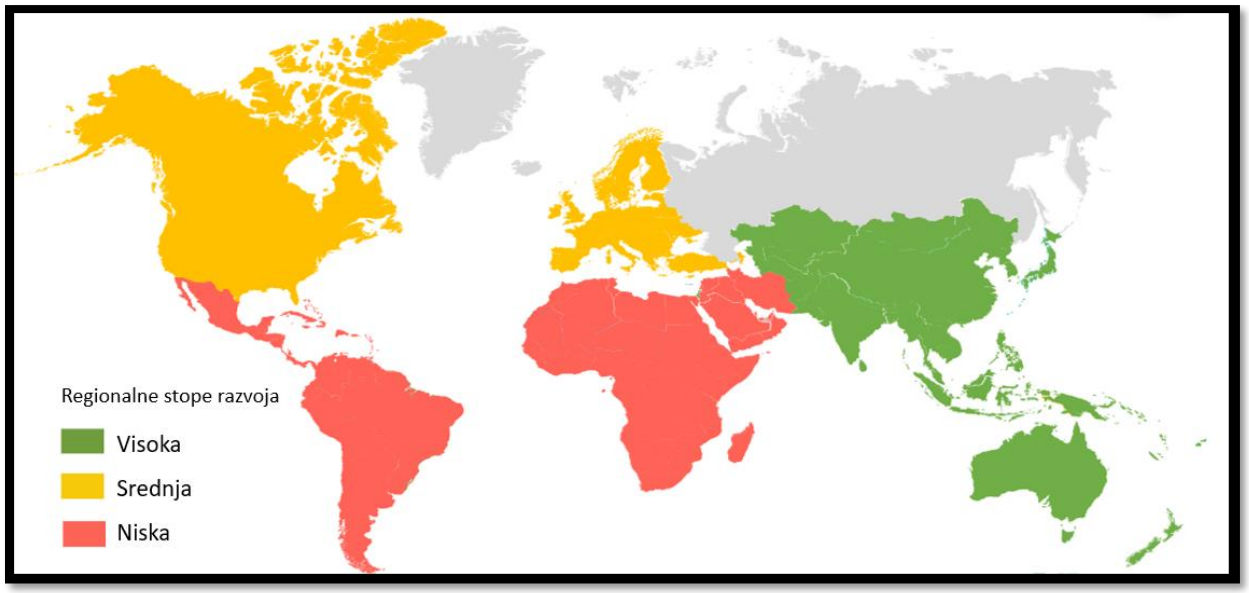
- Simulacija i obuka u području kibernetičke sigurnosti,
- Umjetna inteligencija (*Artificial Intelligence* – AI),
- Detaljna kontrola pristupa,
- Zaštita od bespilotnih letjelica,
- Zaštita infrastrukture zračnog prometa,
- Kibernetičko-fizička sigurnost i situacijska svjesnost, itd.

Neki od glavnih inovativnih projekata su [37]:

- Umjetna inteligencija (*Artificial Intelligence)*
  Poboljšava performanse obrambenih sustava predstavljajući dodatan, kognitivni sloj koji je u mogućnosti identificirati slabosti sustava, doprinijeti poboljšanju stope detekcije napada i razviti kibernetičko-otporni sustav;
- *CitySCAPE*
  Poboljšanje kibernetičke zaštite na razini intermodalnog transporta proizvodnjom *software*-a koji će moći detektirati sumnjivi promet i protok podataka, procijeniti tehnološki i financijski utjecaj kibernetičkih napada te poboljšati protok podataka između relevantnih nadležnih tijela;
- *CONCORDIA/ Cyber Security Competence Network*
  Grupa za razvijanje rješenja za kibernetičku zaštitu, organiziranje panela i konferencija, povezivanje sudionika u zračnom prometu, profesionalnu edukaciju za kibernetičku zaštitu, itd.;
- *CyberRange*
  Razvijanje platforme koja bi omogućila simuliranje složenih realističnih situacija (kao što su kibernetički napadi);

- *ECYSAP (European Cyber Situational Awareness Platform)*
  Europski istraživački projekt sufinanciran od strane Europske komisije i ministara obrane Francuske, Italije, Španjoske i Estonije s ciljem razvijanja platforme koja će utjecati na podizanje svijesti i omogućiti brze metode obrane sustave;
- *IoT Security*
  Omogućavanje zaštite internetske mreže ojačavanjem sigurnosnih ograničenja na svim komunikacijskim kanalima te individualnom autentifikacijom pojedinih uređaja te temeljne sigurnosne provjere nepoznatih internetskih protokola;
- *SATIE (Security of Air Transport Infrastructure of Europe)*
  Projekt specijaliziran za borbu s kibernetičkim prijetnjama na europskim zračnim lukama koji nudi cjelovit pristup prevenciji i detekciji prijetnji te odgovoru na prijetnje i ublažavanju posljedica.

Navedeni inovativni sustavi imati će utjecaj na tržište kibernetičke zaštite u zrakoplovstvu na koje će se po razvitku i plasirati. Stope razvoja tržišta po pojedinim regijama prikazane su na slici 5.



Slika 5. Prognozirane stope razvoja tržišta do 2024. godine
Izvor: *[28]*

S obzirom na žurnost i značaj zaštite kritične infrastrukture civilnog zrakoplovstva, kao i informacijskih i komunikacijskih sustava i podataka od kibernetičkih prijetnji, ICAO (*International Civil Aviation Organization*) je pokrenuo inicijativu za razvoj okvira kibernetičke zaštite u zrakoplovnoj industriji. Na 40. sjednici skupštine ICAO usvojena je Rezolucija A40-10 – Kibernetička zaštita u civilnom zrakoplovstvu. U rezoluciji je naglašena važnost i žurnost zaštite kritične infrastrukture civilnog zrakoplovstva od kibernetičkih prijetnji, te provođenja ICAO strategije kibernetičke sigurnosti u svim državama članicama. [38]

Vizija globalne kibernetičke sigurnosti, prema ICAO-u podrazumijeva snažan sektor civilnog zrakoplovstva otporan na kibernetičke napade, siguran i pouzdan na globalnoj razini, koji se treba kontinuirano razvijati. Ciljevi se mogu postići na sljedeće načine:

- Države članice poštuju svoje obaveze u skladu sa Konvencijom o međunarodnom civilnom zrakoplovstvu (*Chicago Convention*) da bi se osigurali sigurnost i kontinuitet civilnog zrakoplovstva, posebno u vidu kibernetičke sigurnosti,
- Koordinacija ključnih pitanja kibernetičke sigurnosti između država članica da bi se osiguralo provođenje mjera efikasnog upravljanja kibernetičkim rizicima,
- Posvećenost svih interesnih strana razvoju kibernetičke otpornosti, i zaštiti od kibernetičkih napada koji mogu ostaviti negativne posljedice na sigurnost i kontinuitet poslovanja sustava zračnog prijevoza.

Ciljevi ICAO strategije će se postići provođenjem niza principa, mjera i aktivnosti u sklopu okvira zasnovanog na sedam ključnih pretpostavki:

1. Međunarodna suradnja – Kibernetička sigurnost i zrakoplovstvo zahtijevaju suradnju na nacionalnoj i međunarodnoj razini i traže zajedničke aktivnosti pri razvoju, održavanju i unaprjeđenju kibernetičke sigurnosti s ciljem zaštite sektora civilnog zrakoplovstva od svih vrsta kibernetičkih prijetnji sigurnosti sektora. Mjere kibernetičke sigurnosti zrakoplovstva trebaju biti usklađene na globalnoj, regionalnoj i nacionalnoj razini da bi se unaprijedila globalna povezanost i osigurala cjelovita suradnja u provođenju zaštitnih mjera i funkcioniranje sustava upravljanja rizikom.
2. Upravljanje – Države članice bi trebale razviti jasne sustave upravljanja kibernetičkom sigurnošću civilnog zrakoplovstva na nacionalnoj razini. Organizacije upravljanja civilnim zrakoplovstvom bi trebale osigurati koordinaciju sa nacionalnim tijelima odgovornim za kibernetičku sigurnost. Važno je i uspostavljanje adekvatnih kanala komunikacije između različitih vlasti i interesnih strana u sektoru civilnog zrakoplovstva.

3. Efikasne zakonske regulative – Države članice moraju osigurati donošenje i primjenu adekvatne zakonske regulative prije implementacije nacionalne politike o kibernetičkoj sigurnosti u civilnom zrakoplovstvu. Za te svrhe ICAO je kreirao odgovarajuće smjernice vezane za kibernetičku sigurnost koje bi se trebale implementirati u regulative o sigurnosti u civilnom zrakoplovstvu. Države članice bi također trebale ratificirati ICAO instrumente, uključujući Konvenciju o sprječavanju nelegalnih aktivnosti usmjerenih na međunarodno civilno zrakoplovstvo (*Beijing Convention*) i Protokol u sklopu Konvencije za sprječavanje nelegalnog otuđenja zrakoplova (*Beijing Protocol*).
4. Politike kibernetičke sigurnosti – Kibernetička sigurnost je sastavni dio okvira za sveobuhvatno upravljanje rizicima za sigurnost u civilnom zrakoplovstvu. Politike kibernetičke sigurnosti mogu uključivati elemente poput: kulture kibernetičke sigurnosti, promoviranje sigurnosti u fazi dizajna, sigurnost opskrbnih lanaca za softver i hardver, integritet podataka, adekvatne kontrole pristupa podatcima, proaktivno upravljanje ranjivostima sustava, poboljšanje agilnosti u sigurnosnim ažuriranjima bez kompromitiranja sigurnosti, kao i implementiranje sustava i procesa za nadzor podataka od važnosti za kibernetičku sigurnost.
5. Razmjena informacija – Civilno zrakoplovstvo je globalno međuzavisan sustav koji je podložan brzom širenju kibernetičkih napada koji mogu imati globalne negativne efekte. Razmjena informacija bi trebala omogućiti prevenciju, rano otkrivanje i ublažavanje kibernetičkih incidenata prije nego dovedu do većeg narušavanja sigurnosti civilnog zrakoplovstva. Razmjena informacija na polju ranjivosti, prijetnji, incidenata i najboljih praksi, putem uspostavljenih pouzdanih kanala komunikacije mogu uveliko smanjiti negativne efekte napada.
6. Upravljanje incidentima i interventni planovi – Neophodno je razviti adekvatne i prilagodljive planove koji će osigurati kontinuitet zračnog prijevoza tijekom kibernetičkih napada. Testiranje sustava kibernetičke sigurnosti je koristan alat za provjeru kibernetičke otpornosti i identifikaciju prostora za poboljšanje.
7. Jačanje kapaciteta, obuka i kultura kibernetičke sigurnosti – Ljudski faktor je ključni element kibernetičke sigurnosti. Izuzetno je važno da sektor civilnog zrakoplovstva poduzme korake ka unaprjeđenju kvalifikacija i znanja osoblja u vidu kibernetičke sigurnosti. Ovo se može postići podizanjem svijesti o kibernetičkoj sigurnosti, edukacijom, regrutiranjem i obukom. Jačanje vještina vezanih za kibernetičku sigurnost, kako kod postojećeg tako i kod novog osoblja treba se odvijati kontinuirano i u skladu s inovacijama iz svijeta kibernetičke sigurnosti.

5.1. Umjetna inteligencija (AI)

Uz pomoć umjetne inteligencije moguće je brže otkriti zone ranjivosti sustava, te pojačati sustav obrane na dan samog napada. Strojno učenje (*machine learning*), na primjer, može pomoći u detektiranju napada koji nikad ranije nisu viđeni, i na taj način osigurati da je obrana sustava jedan korak ispred napadača. Također, umjetna inteligencija se smatra najefikasnijom u borbi protiv kibernetičkih napada. Iako još nije dovoljno razvijena da bi zamijenila ljudski faktor, AI je vrlo korisna u podršci ljudskim naporima u području kibernetičke zaštite, te pomaže u donošenju boljih odluka za jačanje obrambenog sustava [39].

U budućnosti kibernetičke zaštite, moguća je hibridna strategija koja zamjenjuje alate poput VPN-a i vatrozida sa novom generacijom AI koja ima sposobnosti sveobuhvatne sigurnosne zaštite, pružanja pristupa blokiranim sadržajima, te zaštite od malicioznih sadržaja i *phishing* napada.

5.2. CitySCAPE

CitySCAPE uvodi inovativne tehnike analize rizika i stvara brojna softverska rješenja za realizaciju interoperabilnog alata koji se neprimjetno integrira u bilo koji multimodalni transportni sustav.

Točnije, softverski alat CitySCAPE će biti u mogućnosti:

- Otkriti sumnjive vrijednosti prometnih podataka i identificirati kontinuirane kibernetičke prijetnje,
- Procijeniti učinak kibernetičkog napada u tehničkom i financijskom smislu,
- Kombinirati eksterna znanja i interno promatrane aktivnosti kako bi poboljšao predvidljivost kibernetičkih napada,
- Detektirati umreženo preklapanje kako bi dostavio informativne obavijesti relevantnim službama i podržao njihovo međusobno djelovanje [40].

5.3. CONCORDIA/ Mreža kibernetičke sigurnosti

Konzorcij diljem EU-a koji uključuje istaknutu industriju, akademsku zajednicu, mala i srednja poduzeća i posebno nacionalne centre za kibernetičku zaštitu pokrenuo je projekt H2020 CONCORDIA (*Cyber Security Competence for Research and Innovation*). CONCORDIA planira uvesti „*Cybersecurity Competence Network*“ u EU, kako bi osigurala tehnološko, društveno i političko vodstvo za Europu. CONCORDIA ima za cilj implementirati zajednički Plan istraživanja i inovacija kibernetičke zaštite za Europu.

CONCORDIA je četverogodišnji multidisciplinarni istraživački i inovacijski projekt koji će imati vodeću ulogu u jačanju učinkovitosti sigurnosne unije EU-a. Projektom, koji je započeo u siječnju 2019., koordinira istraživački institut CODE sa Sveučilišta Bundeswehr München i uključuje ukupno 46 partnera. Konzorcij uključuje 23 partnera iz industrije i drugih organizacija te 23 partnera iz akademske zajednice.

CONCORDIA će pomoći Europi da ojača svoje sposobnosti zaštite i osigura svoje digitalno društvo, gospodarstvo i temeljna načela društva za sigurnost i privatnost podataka. CONCORDIA usvaja uključiv pristup, njegujući širok savez koji obuhvaća europsko istraživanje, industriju i javni sektor, uključujući ključne stručnjake iz različitih područja. Razvijanjem inovativnih, tržišnih rješenja za zaštitu Europe od kibernetičkih napada, CONCORDIA će kapitalizirati jedinstveni skup europskih vještina i talenata u području ICT-a i kibernetičke zaštite kako bi uspostavila europski obrazovni ekosustav za kibernetičku zaštitu. Projekt je temeljni instrument za promicanje izvrsnih istraživanja, tržišnih inovacija, izgradnje vještina i istraživački putokaz za kibernetičku zaštitu u Europi [41].

5.4. CyberRange

CyberRange služi kao virtualno okruženje za fleksibilnu simulaciju kritičnih digitalnih IT sustava s različitim komponentama sustava i korisničkim strukturama. Omogućuje sigurno i realistično okruženje za analizu i testiranje incidenata u različitim, skalabilnim scenarijima bez upotrebe originalnih proizvodnih sustava sudionika. Stoga je moguće testirati i potvrditi zaštitne mjere, provjeriti otpornost različitih IT arhitektura kao i uvježbati različite zaštitne procese u poduzeću i specifične procese odgovora na incidente za kibernetičke incidente u realnim scenarijima primjene kako bi se podržala zaštita dizajnerskim pristupima za IT implementacije u

stvarnom svijetu i osiguravanje dosljednih IT operacija za najveću otpornost na kibernetičke napade.

CyberRange:

- cilja na IT sustave i arhitekture specifične za korisnika,
- fokusira se na današnje prijetnje i današnje ICT sustave,
- predviđa prijetnje sutrašnjice i ICT sustave sljedeće generacije,
- pruža uvid u to kako nove tehnologije i procesi mogu poboljšati odgovor na kibernetičke incidente,
- podržava siguran i zaštićen rad industrijskih kontrolnih sustava (*Industrial Control Systems* – ICS) [42].

5.5. ECYSAP

Glavni cilj ECYSAP-a je razviti i implementirati inovativne teorijske osnove, metode i istraživačke prototipove integrirane u pružanje europske operativne platforme za omogućavanje svijesti o kibernetičkim napadima (*Cyber Situational Awareness* – CSA) u stvarnom vremenu s obrambenim sposobnostima brzog odgovora i potporom za donošenje odluka za krajnje korisnike. Plan je razviti integriranu i modularnu platformu za nacionalne/europske sigurnosne svrhe i vojne ekspedicijske operacije, koja će postati obrambeni sustav u stvarnom vremenu s mogućnostima kibernetičkog odgovora, automatiziran i razmjestiv u područjima operacija (nacionalno/europsko) međusobno povezanih između inteligentnih čvorova.

ECYSAP planira dizajnirati, implementirati i potvrditi skup alata analitičkih pokretača za podršku identifikaciji rizika, procjeni i projektiranju procjene njegovog širenja na razini CIS-a i misije. ECYSAP podržava aktivnosti uključene u reaktivne/proaktivne odgovore, uključujući identifikaciju, odabir, planiranje i provedbu smjerova djelovanja (*Courses of Action* – CoA) na razini CIS-a/misije, izvodeći također simulacije i predviđanja operativnog okruženja i CoA-a u različitim vremenskim intervalima (kratkoročni, srednjoročni, dugoročni opseg).

ECYSAP planira dizajnirati, razviti i potvrditi sposobnosti koje olakšavaju razmjenu informacija i izvješćivanje na tehničkoj razini ili razini misije i između obje. Biti će moguće dijeljenje informacija o prijetnjama i utjecajima na misije, nudeći korisniku jednostavne načine pristupa relevantnim i jasnim informacijama. To će sudionicima omogućiti dijeljenje svih vrsta

informacija (incidente, prijetnje, rizike, utjecaje, analize, itd.) i donošenje odluka na suradnički i sinkroniziran način prema unaprijed definiranim procesima rada.

Sposobnosti ECYSAP platforme i njenih komponenti za djelotvoran rad u stvarnoj operativnoj domeni bit će potkrijepljene iscrpnim validacijskim testovima i demonstracijama na stvarnim slučajevima upotrebe koje izravno podržavaju ugrožene države članice EU. Aktivnosti provjere valjanosti provodit će se u virtualnim laboratorijima, testnim platformama, uključujući scenarije bijele/sive/crne kutije protiv automatiziranih suparničkih radnji i timova za čitanje [43].

5.6. IoT

IoT (*Internet of Things*) eksponencijalno raste, ali sigurnost za IoT projekte i implementacije ostaje prepreka za mnoge organizacije. Jedna temeljna IoT sigurnosna komponenta osigurava da uređaji i usluge imaju pouzdane identitete koji mogu komunicirati unutar zaštićenih ekosustava.

Jednostavni certifikati ne mogu se pozabaviti višestrukim razinama ovlaštenja, uloga i informacija koje su potrebne ovim složenim okruženjima. Usvajanjem robusne, upravljane PKI usluge, organizacije mogu pripremiti svoje uređaje za ispunjavanje ovih zahtjeva na zaštićeniji način i po nižoj cijeni nego kod kuće.

IoT uključuje:

- Pouzdane ekosustave i uzajamnu autentifikaciju,
- Funkcije identiteta uređaja,
- Osnove kriptografije s javnim ključem,
- Omogućavanje identiteta uređaja, te
- Prednosti Intertrust PKI kao upravljane PKI usluge [44].

5.7. SATIE

SATIE usvaja holistički pristup prevenciji prijetnji, otkrivanju, odgovoru i ublažavanju u zračnim lukama, istovremeno jamčeći zaštitu kritičnih sustava, osjetljivih podataka i putnika. Kritična imovina obično je zaštićena od pojedinačnih fizičkih ili kibernetičkih prijetnji, ali ne i od složenih scenarija koji kombiniraju obje kategorije prijetnji. Kako bi se nosio s tim, SATIE

razvija interoperabilni alat koji poboljšava cyber-fizičke korelacije, forenzičke istrage i dinamičku procjenu utjecaja u zračnim lukama. Imajući zajedničku svijest o situaciji, stručnjaci za zaštitu i upravitelji zračnih luka učinkovitije surađuju u rješavanju krize. Postupci za hitne slučajeve mogu se istovremeno pokrenuti putem sustava za uzbunjivanje kako bi se promijenio raspored operacija u zračnoj luci, obavijestile osobe koje prve reagiraju, odnosno timovi za kibernetičku zaštitu i timovi za održavanje u cilju brzog oporavka.

Inovativna rješenja bit će integrirana na platformu za simulaciju kako bi se poboljšala njihova interoperabilnost i potvrdila njihova učinkovitost. Provest će se tri demonstracije u različitim dijelovima Europe kako bi se ocijenila rješenja u radnim uvjetima. Rezultati i najbolje prakse bit će široko distribuirani znanstvenoj zajednici, tijelima za standardizaciju, sudionicima u zaštiti i zrakoplovnoj zajednici [45].

6. ZAKLJUČAK

Provođenje brojnih mehanizama rezultiralo je time da se zračni promet smatra jednim od najsigurnijih vrsta prometa, Tome su prethodile brojne međunarodne regulative kao što su Pariška, Varšavska, Čikaška i Montrealska konvencija. Na globalnoj razini važeći su aneksi ICAO-a (njih 19), od kojih se Aneks 17 odnosi specifično na zaštitu civilnog zrakoplovstva, što uključuje i mjere vezane uz kibernetičku zaštitu. Zatim su uslijedili propisi i regulative na europskoj razini, koje je Republika Hrvatska (kao članica EU od 1.7.2013.) bila dužna provesti i implementirati u nacionalno zakonodavstvo. Od europske regulative vezane uz kibernetičku zaštitu, po važnosti je bitno istaknuti Provedbenu uredbu komisije (EU) 2015/1998 i (EU) 2019/1583 te NIS Direktivu.

Iako su standardizirane mjere propisane zakonima i uredbama, u praksi je stanje drugačije jer zračni prijevoznici, zračne luke, pružatelji usluga zračne plovidbe i ostali sudionici u zračnom prometu prilagođavaju zaštitne mjere posebno štiteći vlastite kritične sustave. Sudionici zračnog prometa razlikuju se i po intenzitetu napada pa je tako većina napada usmjerena na zračne prijevoznike (čak 61% svih registriranih napada), a trostruko manje ciljani su proizvođači zrakoplova, zatim slijede zračne luke i ostali sudionici u zračnom prometu.

Jedan od mehanizama upravljanja kibernetičkim rizicima je i sustavno sakupljanje podataka o već provedenim napadima, vrsti napada, napadačima i slično. Analiza tih podataka ukazuje na ranjivosti pojedinog sudionika u zračnom prometu tj. njegove kritične sustave pa je lakše provoditi ciljane mjere zaštite. Stoga se preventivne mjere mogu definirati i po segmentima sustava na koje se odnose; rad na daljinu, mobilne uređaje, informacijsku sigurnost u upravljanju projektima, podjelu dužnosti, itd.

Sljedeći bitan mehanizam u upravljanju kibernetičkim rizicima jest rad na stvaranju inovativnih sustava koji će držati korak s razvojem tehnologije, a time i efektivnije detektirati potencijalne sigurnosne proboje, zaštititi sustave i odgovoriti na rastući broj kibernetičkih napada. Ti inovativni projekti obuhvaćaju područja kao što su detaljna kontrola pristupa, zaštita od bespilotnih letjelica, zaštita infrastrukture zračnog prometa i brojna druga. Ovakvi projekti zahtjevaju unosna ulaganja, a na njihovoj realizaciji surađuju gotovo svi sudionici zračnog prometa.

Zaključak jest da samo kombinacija provođenja zakonske regulative i primjena iste u praksi, precizne mjere zaštite i ulaganje u inovativne sustave zaštite mogu osigurati nužnu razinu kibernetičke zaštite u zračnom prometu.

LITERATURA

1. Peace Palace Library. *Air Law*. Preuzeto s: https://peacepalacelibrary.nl/research-guide/air-law [Pristupljeno: 11. kolovoza 2022.]

2. Hrvatska enciklopedija. *Zračno pravo*. Preuzeto s: https://enciklopedija.hr/natuknica.aspx?id=67450 [Pristupljeno: 11. kolovoza 2022.]

3. Struna – Hrvatsko strukovno nazivlje. *Konvencija o međunarodnome civilnom zrakoplovstvu*. Preuzeto s: http://struna.ihjj.hr/naziv/konvencija-o-medjunarodnome-civilnom-zrakoplovstvu/1607/ [Pristupljeno: 11. kolovoza 2022.]

4. Steiner S. *Preventivne zaštitne mjere – Kibernetička zaštita*. [Prezentacija] Zaštita u zračnom prometu. Fakultet prometnih znanosti Sveučilišta u Zagrebu, 2021.

5. ICAO. *Annex 17 – Aviation Security*. Preuzeto s: https://www.icao.int/security/sfp/pages/annex17.aspx [Pristupljeno: 11. kolovoza 2022.]

6. International Civil Aviation Organization. *Annex 17 to the Convention on International Civil Aviation*. Preuzeto s: https://skylibrarys.files.wordpress.com/2016/07/annex-17-security.pdf [Pristupljeno: 11. kolovoza 2022.]

7. Europski parlament i Vijeće Europske unije. *Uredba (EU) 2018/1139 Europskog parlamenta i Vijeća. Izadnje: 212/1*. Strasbourg: Službeni list Europske unije; 2018.

8. European Union. *European Union Aviation Safety Agency (EASA)*. Preuzeto s: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/easa_en [Pristupljeno: 11. kolovoza 2022.]

9. Europska komisija. *Provedbena uredba komisije (EU) 2015/1998 o utvrđivanju detaljnih mjera za provedbu zajedničkih osnovnih standarda iz područja zaštite zračnog prometa. Izdanje: 299/1*. Bruxelles: Službeni list Europske unije; 2015.

10. Europska komisija. *Provedbena uredba komisije (EU) 2019/1583 o izmjeni Provedbene uredbe (EU) 2015/1998 o utvrđivanju detaljnih mjera za provedbu zajedničkih osnovnih standarda iz područja zaštite zračnog prometa u pogledu mjera kibersigurnosti. Izdanje: 246/15*. Bruxelles: Službeni list Europske unije; 2019.

11. Ministarstvo unutarnjih poslova - Ravnateljstvo civilne zaštite. *Kritična infrastruktura*. Preuzeto s: https://civilna-zastita.gov.hr/kriticna-infrastruktura/111 [Pristupljeno: 11. kolovoza 2022.]

12. Europski parlament i Vijeće Europske unije. *Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije. Izdanje: 194/1*. Strasbourg: Službeni list Europske unije; 2016.

13. Europski parlament i Vijeće Europske unije. *Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002. Izdanje: 97/72*. Strasbourg: Službeni list Europske unije; 2008.

14. Europski parlament i Vijeće Europske unije. *Direktiva 2009/12/EZ Europskog parlamenta i Vijeća o naknadama zračnih luka. Izdanje: 70/11*. Strasbourg: Službeni list Europske unije; 2009.

15. Republika Hrvatska. *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Izdanje: 1305*. Zagreb: Narodne novine; 2018.

16. Republika Hrvatska. *Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Izdanje: 1399*. Zagreb: Narodne novine; 2018.

17. CERT. *Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga (u skladu sa Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga)*. Preuzeto s: https://www.cert.hr/wp-content/uploads/2018/11/Smjernice-za-dostavu-obavijesti-o-incidentima-sa-znatnim-u%C4%8Dinkom-operatora-klju%C4%8Dnih-usluga-i-davatelja-digitalnih-usluga-2.pdf [Pristupljeno: 11. kolovoza 2022.]

18. Stastny P, Stoica AM. Protecting aviation safety against cybersecurity threats. *IOP Conference Series: Materials Science and Engineering*. 2022;1226: 1-8. Preuzeto s: https://iopscience.iop.org/article/10.1088/1757-899X/1226/1/012025/pdf [Pristupljeno: 11. kolovoza 2022.]

19. Republika Hrvatska. *Odluka o donošenju Nacionalnog programa sigurnosti u zračnom prometu. Izdanje: 2632*. Zagreb: Narodne novine; 2015.

20. EUROCONTROL EATM-CERT Services. *Think Paper #12 - Aviation under attack from a wave of cybercrime*. Preuzeto s: https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cybercrime [Pristupljeno: 11. kolovoza 2022.]

21. Documents. *Aviation perspectives 2016 special report series: Cybersecurity and the airline industry*. Preuzeto s: https://fdocuments.in/document/2016-special-report-series-cybersecurity-and-the-perspectives-2016-special.html?page=1 [Pristupljeno: 12. kolovoza 2022.]

22. Lufthansa Technik. *In-flight Entertainment & Connectivity - Connected to the world*. Preuzeto s: https://www.lufthansa-technik.com/inflight-entertainment-connectivity [Pristupljeno: 12. kolovoza 2022.]

23. Wolf M, Minzlaff M, Moser M. Information Technology Security Threats to Modern e-Enabled Aircraft: A Cautionary Note. *Journal of Aerospace Computing, Information and Communication*. 2014;11(7): 447-457. Preuzeto s: https://www.researchgate.net/publication/277674971_Information_Technology_Security_Threats_to_Modern_e-Enabled_Aircraft_A_Cautionary_Note [Pristupljeno: 12. kolovoza 2022.]

24. cnsight. *Top 5 Cyber Attacks in the Aviation Industry*. Preuzeto s: https://cnsight.io/2021/04/16/top-5-cyber-attacks-in-the-aviation-industry/ [Pristupljeno: 12. kolovoza 2022.]

25. Gopalakrishnan K, Govindarasu M, Jacovson DW, Phares BM. Cyber security for airports. *International Journal for Traffic and Transport Engineering*. 2013;3(4): 365-376. Preuzeto s: https://www.researchgate.net/publication/274123014_CYBER_SECURITY_FOR_AIRPORTS [Pristupljeno: 12. kolovoza 2022.]

26. Civil Air Navigation Services Organisation. *CANSO Cyber Security and Risk Assessment Guide*. Preuzeto s: https://www.dhmi.gov.tr/Lists/SsdHavaTrafikSbMd_KurumsalBilveDoc/Attachments/131/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf [Pristupljeno: 12. kolovoza 2022.]

27. nsfocus. *Cybersecurity of Clouds over 10,000 Meters*. Preuzeto s: https://nsfocusglobal.com/cybersecurity-of-clouds-over-10000-meters/ [Pristupljeno: 12. kolovoza 2022.]

28. Mordor Intelligence. *Aviation CyberSecurity Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027)*. Preuzeto s: https://www.mordorintelligence.com/industry-reports/global-aviation-cyber-security-market [Pristupljeno: 12. kolovoza 2022.]

29. Ukwandu E, Farah MAB, Hindy H, Bures M, Atkinson RC, Tachtatzis C, Bellekens X. *Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends*. Preuzeto s: https://www.researchgate.net/publication/353208515_Cyber-

Security_Challenges_in_Aviation_Industry_A_Review_of_Current_and_Future_Trends [Pristupljeno: 12. kolovoza 2022.]

30. Europska unija. *Agencija Europske unije za kibernetičku sigurnost (ENISA)*. Preuzeto s: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_hr [Pristupljeno: 12. kolovoza 2022.]

31. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2021*. Preuzeto s: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 [Pristupljeno 12. kolovoza 2022.]

32. European Union Agency for Cybersecurity. *ENISA Threat Landscape for Ransomware Attacks*. Preuzeto s: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks [Pristupljeno: 13. kolovoza 2022.]

33. AVIATION ISAC. *2022 Cyber Risk Survey*. Preuzeto s: https://www.a-isac.com/reports [Pristupljeno: 13. kolovoza 2022.]

34. iso.org. *International Organization for Standardization*. Preuzeto s: https://www.iso.org/home.html [Pristupljeno: 13. kolovoza 2022.]

35. iso.org. *ISO/IEC 27001 Information security management*. Preuzeto s: https://www.iso.org/isoiec-27001-information-security.html [Pristupljeno: 13. kolovoza 2022.]

36. isms.online. *ISO 27001 – Annex A.6: Organisation of Information Security*. Preuzeto s: https://www.isms.online/iso-27001/annex-a-6-organisation-information-security/ [Pristupljeno: 13. kolovoza 2022.]

37. Airbus cybersecurity. *Innovation*. Preuzeto s: https://airbus-cyber-security.com/products-and-services/innovation/ [Pristupljeno: 13. kolovoza 2022.]

38. ICAO. *A40-10: Addressing Cybersecurity in Civil Aviation*. Preuzeto s: https://www.icao.int/cybersecurity/Documents/A40-10.pdf [Pristupljeno: 20. kolovoza 2022.]

39. Udemy. *Artificial Intelligence risk and cyber security*. Preuzeto s: https://www.udemy.com/course/artificial-intelligence-ai-governance-and-cyber-security/ [Pristupljeno: 20. kolovoza 2022.]

40. CitySCAPE. *The CitySCAPE Solution*. Preuzeto s: https://www.cityscape-project.eu/ [Pristupljeno: 20. kolovoza 2022.]

41. CONCORDIA. *Cybersecurity Competence Network*. Preuzeto s: https://www.concordia-h2020.eu/news/concordia-cybersecurity-competence-network-press-release/ [Pristupljeno: 20. kolovoza 2022.]

42. AIT. *Cyber Range*. Preuzeto s: https://cyberrange.at/ait-cyber-range/ [Pristupljeno: 20. kolovoza 2022.]

43. ECYSAP. *Concept and approach*. Preuzeto s: https://www.ecysap.eu/concept.html [Pristupljeno: 20. kolovoza 2022.]

44. Intertrust. *IoT Security*. Preuzeto s: https://www.intertrust.com/resources/ [Pristupljeno: 20. kolovoza 2022.]

45. SATIE. *Security of Air Transport Infrastructure of Europe*. Preuzeto s: https://satie-h2020.eu/index.php/about/ [Pristupljeno: 20. kolovoza 2022.]

POPIS KRATICA

ICAO	(International Civil Aviation Organization) Organizacija međunarodnog civilnog zrakoplovstva
SARPs	(Standards and Recommended Practices) Standardi i preporučene prakse
EU	(European Union) Europska Unija
NIS Direktiva	(Directive on security of network and information systems) Direktiva o sigurnosti mrežnih i informacijskih sustava
EASA	EASA (European Union Aviation Safety Agency) Agencija Europske unije za sigurnost zračnog prometa
CSIRT	(Computer Security Incident Response Team) Tim za odgovor na računalne sigurnosne incidente
SMS	(Safety Management System) Sustav upravljanja sigurnošću
NIST	(National Institute of Standards and Technology) Nacionalni Institut za standarde i tehnologiju
ANSP	(Air Navigation Service Provider) Pružatelj usluga u zračnoj plovidbi
EFBs	(Electronic Flight Bags) Elektroničke letačke torbe
IFEC	(In-flight Entertainment & Connectivity) Sustavi za zabavu tijekom leta
GPS	(Global Positioning System) Globalni sustav za određivanje položaja
GPRS	(General Packet Radio Service) Opća radiousluga za prijenos datoteka
GSM	(Global System for Mobile Communications) Globalni sustav za mobilne telekomunikacije
SITA	(Société Internationale de Télécommunications Aéronautiques) Međunarodna kompanija za pružanje zrakoplovnih telekomunikacija
USB	(Universal Serial Bus) Prijenosna memorijska jedinica
BYOD	(Bring Your Own Device) Donesi vlastiti uređaj
A-ISAC	(Aviation Information Sharing and Analysis Center) Centar za dijeljenje i analizu zrakoplovnih informacija
DDoS	(Distributed Denial of Service) Distribuirani napadi uskraćivanjem usluga
TLP	(Traffic Light Protocol) Protokol semaforskih svjetala

ENISA	(European Union Agency for Cybersecurity) Agencija Europske unije za kibernetičku sigurnost
ETL	(ENISA Threat Landscape) ENISA pregled prijetnji
OEM	(Original Equipment Manufacturers) Proizvođači originalne opreme
IDM	(Identity Management) Upravljanje identitetima
IPPP	(Information Protection Processes and Procedures) Procesi i postupci zaštite informacija
SOC	(Security Operations Center) Centar za operativnu sigurnost
ISO	(International Organization for Standardization) Međunarodna organizacija za normizaciju
IEC	(International Electrotechnical Commission) Međunarodno elektrotehničko povjerenstvo
ISMS	(Information Security Management System) Sustav upravljanja sigurnošću informacija
AI	(Artificial Intelligence) Umjetna inteligencija
PSS	(Passenger Service System) Sustav usluga za putnike
VPN	(Virtual Private Network) Virtualna privatna mreža
ICT	(Information and Communications Technology) Informacijska i komunikacijska tehnologija
ICS	(Industrial Control Systems) Industrijski kontrolni sustavi
CSA	(Cyber Situational Awareness) Svijest o kibernetičkim napadima
CoA	(Courses of Action) Smjerovi djelovanja
PKI	(Public Key Infrastructure) Infrastruktura javnog ključa
DPIA	(Data Protection Impact Assessments) Procjena učinka na zaštitu podataka
GDPR	(General Data Protection Regulation) Opća uredba o zaštiti podataka

POPIS SLIKA

POPIS TABLICA

POPIS GRAFIKONA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je **ZAVRŠNI RAD**
(vrsta rada)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da 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/diplomskog rada pod naslovom **Upravljanje kibernetičkim rizicima u zrakoplovstvu**, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

Tihana Bogdan

U Zagrebu, 29. kolovoza 2022.

Tihana Bogdan
(ime i prezime, *potpis*)