SUVREMENI KIBERNETIČKI RIZICI U UPRAVLJANJU ZRAČNIM PROMETOM

CONTEMPORARY CYBERSECURITY RISKS IN AIR TRAFFIC MANAGEMENT

Stručni članak

Marija Prskalo, mag.ing.el.[*]

Sažetak

Suvremeno civilno zrakoplovstvo koristi visoko sofisticirane informacijske tehnologije kako bi osiguralo siguran, učinkovit i pouzdan zračni promet. Ova grana industrije ima ključnu ulogu u globalnom povezivanju i prijevozu putnika te tereta. No, s napretkom tehnologije dolazi i povećana složenost sustava, otvarajući vrata različitim izazovima i potencijalnim opasnostima. U kontekstu sve veće povezanosti i digitalizacije zrakoplovnog sektora, naglašava se rizik od kibernetičkih prijetnji u upravljačkim sustavima zračnog prometa. Cilj ovog rada je provesti temeljnu analizu kibernetičkih prijetnji u upravljačkom sustavu zračnog prometa, istražujući ključne aspekte, metodologije procjene rizika i normativne okvire. Dodatno, rad će analizirati međunarodne standarde i preporučene prakse, fokusirajući se na preventivne mjere i metode zaštite kako bi identificirao ključne strategije očuvanja integriteta i sigurnosti sustava. Ovaj pristup odražava nužnost suočavanja s izazovima kibernetičkih prijetnji, pridonoseći stabilnosti i pouzdanosti zračnog prometa.

Ključne riječi: zračni promet, kibernetičke prijetnje, upravljanje rizicima, normativni okvir.

Abstract

Contemporary civil aviation employs highly sophisticated information technologies to ensure safe, efficient, and reliable air traffic. This industry plays a pivotal role in global connectivity and the transportation of passengers

[*] *Agencija za pružanje usluga u zračnoj plovidbi Bosne i Hercegovine, e-mail: marijaprskalo@fkn.unsa.ba*

and cargo. However, technological advancements contribute to increased system complexity, opening doors to various challenges and potential hazards. In the context of the growing interconnectedness and digitization of the aviation sector, the risk of cyber threats in air traffic management systems is emphasized. The aim of this paper is to conduct a comprehensive analysis of cyber threats in the air traffic management system, exploring key aspects, risk assessment methodologies, and regulatory frameworks. Additionally, the paper will analyze international standards and recommended practices, focusing on preventive measures and protection methods to identify key strategies for preserving system integrity and security. This approach reflects the necessity of addressing the challenges posed by cyber threats, contributing to the stability and reliability of air traffic.

Keywords: air traffic, cyber threats, risk management, regulatory framework.

1. UVOD

Sektor zračnog prometa često se opisuje kao kompleksan sektor koji se oslanja na napredne informacijske tehnologije, ključne za postizanje optimalne sigurnosti, učinkovitosti i pouzdanosti zračnog prometa. S porastom povezanosti i digitalizacije, dok se sektor razvija prema višim standardima, suočava se s rastućim izazovom - kibernetičkim prijetnjama. Napadi na sustave upravljanja zračnim prometom nisu samo teoretska prijetnja; posljednjih godina primjećuje se postupni porast takvih incidenata. Kibernetičke prijetnje predstavljaju suptilan, ali izuzetno ozbiljan rizik koji proizlazi iz sveprisutne povezanosti i digitalne infrastrukture zračnog prometa te iz različitih izvora.

Ovaj rad ima za cilj temeljnu analizu kibernetičkih rizika u sustavu upravljanja zračnim prometom, istražujući ključne aspekte, metodologije procjene rizika te normativne okvire koji čine esencijalnu osnovu za sigurnost u ovom izuzetno značajnom sektoru. Svrha rada je pružiti sustavnu klasifikaciju kibernetičkih prijetnji kako bi se stvorio čvrst temelj za razvoj i implementaciju sigurnosnih mjera, od vitalne važnosti u današnjem digitalnom dobu, čime se naglašava imperativ očuvanja stabilnosti i pouzdanosti sustava upravljanja zračnim prometom. Naslovljeno na međunarodne standarde i preporuke, razmatra se kako zaštititi civilno zrakoplovstvo od potencijalnih kibernetičkih napada. Kroz analizu preventivnih mjera i metoda zaštite, od

iznimne je važnosti identificirati ključne strategije koje doprinose očuvanju integriteta i sigurnosti sustava zračnog prometa. Fokus će biti usmjeren na međunarodnu suradnju i norme koje igraju bitnu ulogu u suzbijanju kibernetičkih prijetnji na globalnoj razini. Ovaj pristup odražava nužnost zajedničkih napora u osiguranju kibernetičke otpornosti zračnog prometa, čime se jača ukupna sigurnost i stabilnost ovog ključnog sektora.

2. KLASIFIKACIJA KIBERNETIČKIH RIZIKA

S obzirom na zaštićena dobra i vrijednosti razlikuje se više vrsta sigurnosti, između ostalog, sigurnost prometa na putevima, u zraku, na rijekama i morima, koja se ostvaruje zakonima i drugim propisima kojim su definirana prometna pravila koja određuju ponašanje sudionika, organe koji reguliraju i vrše kontrolu sigurnosti u tim oblastima (Masleša, 2001).
Sustav zračnog prometa dijeli se na:

- infrastrukturu (aerodrome i zračne puteve sa sredstvima koja ih definiraju),
- zrakoplove, odnosno letjelice koje koriste infrastrukturu,
- kontrolu letenja i vođenja zrakoplova (Pavlin, 2006).

Sigurnost je rezultat upravljanja brojnim organizacijskim procesima, koji imaju za cilj da sigurnosne rizike drže pod kontrolom. Ključnu ulogu u tom smislu ima sigurnost, kao rezultat i upravljanje sigurnosnim rizikom, kao proces. Organizacijski aspekt sigurnosti sustava zračnog prometa u užem smislu predstavlja prostornu i vremensku sinkronizaciju niza subjekata i aktivnosti u jedinstven kontinuirani proces (Steiner, 1998). Za sve procese upravljanja vrijede neki opći principi i zakonitosti neovisno o prirodi upravljivog sustava i njegovih ciljeva. Svaki sustav s upravljanjem naziva se kibernetički sustav. Upravljanje se sastoji od izbora više alternativa, odnosno više trajektorija sustava kojima se može stići do unaprijed definiranog cilja (Obradović, 2018). Kibernetička prijetnja manifestira se kroz namjerne ili nenamjerne, ciljane ili ne-ciljane procese, te može proizići iz raznolikih izvora, uključujući vanjske organizacije koje sudjeluju u špijunaži i informacijskim ratovima, kriminalce, hakere te nezadovoljne zaposlenike unutar samih organizacija. Sektor zračnog prometa postaje sve učestalija meta ovakvih prijetnji, a posljednjih godina primjećuje se postupni porast napada na sustave upravljanja zračnim prometom. Dosad su se ti napadi uglavnom usmjeravali

na zračne prijevoznike i proizvodna područja gdje se čuvaju podaci visokog stupnja osjetljivosti. Iako su kibernetički napadi na sustave upravljanja zračnim prometom bili ograničeni, uloga zrakoplovstva na globalnoj razini čini ga prestižnom metom za potencijalne napadače, što povećava vjerojatnost budućih incidenata koji mogu utjecati na ove sustave (CANSO, 2023).

Ciljani napad predstavlja planski pokušaj napada od strane grupe ili pojedinca na ključni infrastrukturni sustav. Suprotno tome, ne-ciljani napad javlja se kada je svrha napada neodređena, kao u slučaju širenja virusa, crva ili zlonamjernog softvera putem interneta bez specifičnog cilja. Prijetnje su općenito klasificirane na one usko povezane s pojedinom organizacijom, šire prijetnje koje imaju za cilj zahvatiti što veći broj organizacija ili pojedinaca te napade usmjerene na infrastrukturu. Ove prijetnje često čine organizacije i pojedince unutar njih nenamjernim žrtvama, koristeći različite tehnike koje postaju sve sofisticiranije. Važno je napomenuti da prijetnje mogu eskalirati ili čak ostvariti svoj potencijal zbog nepažljivosti ili nedostatne obučenosti zaposlenika, nedostataka u operativnim procedurama, neažurirane softverske opreme te kvarova opreme koji nehotice uzrokuju smetnje u računalnim sustavima ili oštećuju podatke.

3. METODOLOGIJA PROCJENE RIZIKA

Metodologija procjene rizika u sustavima upravljanja zračnim prostorom ovisi o različitim parametrima te čini standardan segment procesa upravljanja rizicima unutar organizacije pružatelja usluga. Glavni je cilj prepoznavanje, procjena i smanjenje rizika na najmanju dopuštenu razinu. Upravljanje rizicima pruža temelj za planiranje operacija ili aktivnosti u sektoru zračnog prometa te donošenje odluka, potičući proaktivni pristup umjesto reaktivnog pristupa upravljanja sigurnošću zračne plovidbe. Ovo se postiže sustavnim prikupljanjem i analizom relevantnih informacija kako bi se identificirale opasnosti i uspostavila kontrola rizika već u fazi planiranja operacija. Time se izbjegava suočavanje s neželjenim situacijama nakon što operacije već započnu. Prema Ahić i Nađ (2017) procjena rizika predstavlja postupak u kojem se definira gdje, kada, zašto i kako bi se događaji mogli spriječiti, umanjiti, odgoditi ili povećati postizanje ciljeva. Organizacija nužno treba identificirati izvore rizika, područja utjecaja, događaje i njihove uzroke kao i njihove potencijalne posljedice. Unatoč nemogućnosti potpune eliminacije rizika, većina njih može biti predviđena i učinkovito upravljana. Cilj

upravljanja rizicima jest identificirati relevantne faktore rizika za određeni događaj te razviti plan upravljanja rizicima s ciljem smanjenja vjerojatnosti pojave potencijalno rizičnih čimbenika i/ili njihovog negativnog utjecaja na sigurnost zračne plovidbe. Rizik označava kombinaciju opće vjerojatnoće ili učestalosti pojavljivanja štetnog utjecaja izazvanog opasnošću i ozbiljnost tog utjecaja. U tablici 1. prikazano je značenje ozbiljnosti posljedice događaja i vjerojatnoće događaja.

Tablica 1. Tablica ozbiljnosti posljedica i vjerojatnoće događaja (Izvor: BHDCA, 2014)

OZBILJNOST POSLJEDICA DOGAĐAJA			**VJEROVATNOĆA DOGAĐAJA**		
Definicija u zrakoplovstvu	Značenje	Vrijednost	Kvalitativna definicija	Značenje	Vrijednost
Katastrofalan	Uništena oprema Višestruke smrti	A	Čest	Vjerojatno će se događati često (već se događalo mnogo puta)	5
Hazardan	Krupno smanjenje sigurnosnih margina. Fizičko ili radno opterećenje takvo da se ne može pouzdati u operatore da će obaviti svoje zadatke precizno ili u potpunosti Ozbiljne povrede ili smrt više osoba Veliko oštećenje na opremi	B	Povremen	Vjerojatno će se ponekad javiti (pojavljivao se s vremena na vrijeme)	4
Veći	Značajno smanjenje sigurnosnih margina Smanjenje mogućnosti operatora da se nose s nepovoljnim operativnim uvjetima kao posljedica povećanog radnog opterećenja ili kao rezultat uvjeta koji smanjuju efikasnost operatora Ozbiljni incident Povrijeđene osobe	C	Rijedak	Nije mnogo vjerojatno da će se dogoditi, ali postoji mogućnost (događalo se rijetko)	3
Manji	Smetnja Operativna ograničenja Upotreba emergency procedura Manji incident	D	Malo vjerojatan	Veoma malo vjerojatno da će nastupiti (nije se događalo do sada)	2
Zanemariv	Sitne posljedice	E	Izuzetno nevjerojatan	Gotovo nezamislivo da će se dogoditi	1

Tablica 2. Matrica procjene rizika (Izvor: BHDCA, 2014)

Vjerovatnoća rizika	***Ozbiljnost rizika***				
	Katastrofalan A	Hazardan B	Veći C	Manji D	Zanemarljiv E
Čest – 5	5A	5B	5C	5D	5E
Povremen – 4	4A	4B	4C	4D	4E
Rijedak – 3	3A	3B	3C	3D	3E
Malo vjerovatan – 2	2A	2B	2C	2D	2E
Izuzetno nevjerovatan – 1	1A	1B	1C	1D	1E

Neprihvatljiv pod postojećim uvjetima

Prihvatljivo na osnovu ublažavanja rizika. Može zahtijevati menadžersku odluku

Prihvatljiv

Nakon što se dodijele vrijednosti rizicima korištenjem matrice procjene rizika može se dodijeliti i opseg vrijednosti za kategorizaciju rizika kao prihvatljivi, neželjeni i neprihvatljivi. Ovi termini su objašnjeni na sljedeći način:

- Prihvatljivi rizik znači da nije potrebno poduzimati dalje akcije (osim u slučaju da se rizik može još više reducirati ili potpuno ukloniti sa neznatnim troškovima).
- Neželjeni (ili podnošljivi) rizik znači da su osobe koje su izložene danom riziku spremne da ga prihvate kako bi priuštile određene koristi, pri čemu je rizik smanjen na najmanju prihvatljivu razinu.
- Neprihvatljivi rizik znači da se operacije pod trenutnim uvjetima moraju prekinuti dok se rizik ne reducira bar na prihvatljivu razinu (BHDCA, 2014).

Četiri osnovna principa koja upravljaju svim aktivnostima koje se sprovode u okviru provođenja procesa upravljanja rizikom uključuju:

- prihvaćanje minimalnog sigurnosnog rizika,
- donošenje rizičnih odluka na odgovarajućoj razini upravljanja,
- prihvaćanje sigurnosnog rizika kada dobit nadvladava troškove,
- integriranje upravljanja sigurnosnim rizikom u procesu planiranja na svim razinama upravljanja (Čokorilo, 2020).

4. PROCJENA SIGURNOSTI KIBERNETIČKIH RIZIKA

Rizik kibernetičke sigurnosti predstavlja prijetnju organizacijskim operacijama civilnog zrakoplovstva, imovini, pojedincima i drugim organizacijama zbog potencijala kibernetičkog događaja. U kontekstu

organizacije koja se bavi pružanjem usluga u zračnoj plovidbi odgovarajuća procjena sigurnosti može biti od koristi, s obzirom da se utjecaj na razinu usluga zračnog prometa često već identificira kao sastavni dio sigurnosnog procesa. Kvalitetna procjena sigurnosti kibernetičkih rizika u zračnom prometu obuhvaća:

- utvrđivanje utjecaja napada na povjerljivost, integritet i dostupnost,
- identifikaciju ciljeva napada,
- klasifikaciju napadačkih tehnika kibernetičkog napadača,
- klasifikaciju težine izvodivosti napada,
- razvoj napadačkih „stabala“,
- utjecaj napada (EUROCONTROL, 2013).

Analiza kibernetičkih rizika treba biti što preciznija kako bi se rizik uklonio u što kraćem roku i sa što manjim posljedicama. Analiza treba uključivati plan procjene rizika i evaluaciju eventualnih posljedica na sigurnost sustava u zračnom prometu. Prema Ahić i Nađ (2017) izvođenje kvalitativne analize rizika procjenjuje prioritet utvrđenih rizika koristeći relevantnu vjerojatnoću ili vjerojatnoću pojave, te odgovarajući utjecaj na ciljeve, ako se realiziraju rizici, kao i druge faktore. Nadalje, rezultati kvalitativne analize rizika mogu ukazivati na potrebu ažuriranja dokumentacije, registra rizika i utvrđenih pretpostavki. Dok izvođenje kvantitativne analize rizika predstavlja proces brojčane analize učinka utvrđenih rizika i provodi se za rizike koji su prioritetni prema provedenoj kvalitativnoj analizi rizika. Sve veći trend uvođenja automatizacije u operacije zrakoplova doveo je do sve veće dostupnosti informacijskih i komunikacijskih tehnologija što dovodi u pitanje integritet, povjerljivost i zaštitu podataka. Suvremene informatičke prijetnje u zračnom prometu se konstantno razvijaju, pri čemu je osnova na zlonamjernim prijetnjama, poremećajima u poslovanju i krađi informacija bazirana na političkim, financijskim ili drugim motivima (Čokorilo, 2020). Povjerljivost, integritet i dostupnost podataka predstavljaju ključne ciljeve u sustavu upravljanja zračnim prometom. Povjerljivost osigurava da osjetljivi podaci o zračnom prometu budu zaštićeni od neovlaštenog pristupa ili otkrivanja. Integritet se odnosi na očuvanje točnosti, cjelovitosti i autentičnosti podataka, sprječavajući neovlaštene promjene ili manipulacije. Dostupnost jamči pravovremeni pristup važnim informacijama kada su potrebne, čime se osigurava neprekidnost operacija i sigurnost zračnog prometa. Navedena

načela zajedno čine temelj za pouzdano i sigurno upravljanje podacima u sustavu upravljanja zračnim prometom.

Identifikacija ciljeva napada odnosi se na proces prepoznavanja sustava, mreža ili podataka koji su potencijalno izloženi kibernetičkim prijetnjama. Stoga ovaj korak uključuje analizu mogućih meta napada kako bi se utvrdilo koje informacije ili resursi mogu biti cilj napadača. Identifikacija ciljeva ključna je za pravilno usmjeravanje resursa i implementaciju odgovarajućih sigurnosnih mjera u organizaciji koja se bavi pružanjem usluga. Klasifikacija težine izvodivosti napada odnosi se na procjenu koliko je jednostavno ili teško izvesti određeni kibernetički napad. Stoga aspekt uključuje analizu napadačkih resursa, vještina i sofisticiranosti te procjenu mogućnosti otkrivanja ili sprječavanja napada.

Razvoj napadačkih "stabala" odnosi se na izradu grafikona ili dijagrama koji prikazuju hijerarhiju ili slijednost koraka koje napadač poduzima tijekom kibernetičkog napada. Predmetna tehnika analize pomaže u vizualizaciji načina na koje napadač postepeno prodire u sustav, širi se kroz mrežu ili izvodi druge aktivnosti. Razumijevanje "stabala" napada omogućuje stručnjacima za kibernetičku sigurnost da bolje prepoznaju i razvijaju strategije obrane protiv specifičnih scenarija napada. Utjecaj napada odnosi se na procjenu štete ili posljedica koje kibernetički napad može imati na sustav upravljanja zračnim prometom, organizaciju koja se bavi pružanjem usluga ili pojedinca kao dijela te organizacije. Utvrđivanje stvarnog i potencijalnog utjecaja napada ključno je za donošenje informiranih odluka o sigurnosti, usmjeravanje resursa prema najkritičnijim aspektima sustava te razvoj odgovarajućih strategija zaštite i oporavka. Procjena vjerojatnosti nastanka kibernetičkog rizika ključan je korak u upravljanju sigurnošću sustava za upravljanje zračnim prometom. Proces uključuje analizu različitih faktora kako bi se odredila vjerojatnost da se dogodi određeni kibernetički događaj. Na temelju identificiranih prijetnji, ranjivosti, izloženosti i utjecaja, stručnjaci za sigurnost procjenjuju vjerojatnost nastanka svakog specifičnog kibernetičkog rizika.

Temelj kulture kibernetičke sigurnosti leži u uspostavi i provedbi internog sustava izvješćivanja o kibernetičkoj sigurnosti. Ovaj sustav omogućuje organizacijama koje se bave pružanjem usluga u zračnoj plovidbi proaktivno upravljanje kibernetičkim rizicima, mjerenje napretka u kibernetičkoj sigurnosti te prepoznavanje i planiranje potreba za podizanjem svijesti i obukom zaposlenika. Inicijative koje potiču zaposlenike na prijavu kibernetičkih incidenata, promičući pritom kulturu pravičnosti, od suštinske su

važnosti. Pri izradi mehanizama izvješćivanja o kibernetičkoj sigurnosti, organizacije bi trebale koristiti svoje iskustvo stečeno u razvoju i implementaciji sustava izvješćivanja o sigurnosti u zračnoj plovidbi (ICAO, 2022).

5. NORMATIVNI OKVIR ZAŠTITE ZRAČNOG PROMETA OD KIBERNETIČKIH NAPADA

U kontekstu međunarodne regulative, utvrđivanje minimalnih standarda zrakoplovne sigurnosti na globalnoj razini leži pod nadležnošću Organizacije međunarodnog civilnog zrakoplovstva (ICAO)*. Temeljni ICAO standardi definirani su u 19 Aneksa Čikaške konvencije. Među njima, Aneks 17* posebno se bavi preventivnim mjerama zaštite civilnog zrakoplovstva, uključujući konkretne odredbe usmjerene na kibernetičke opasnosti. Ova regulativa postavlja smjernice i standarde kako bi osigurala globalnu koordinaciju i standardizaciju sigurnosnih praksi u zrakoplovnom sektoru.

Organizacija ICAO tako igra ključnu ulogu u osiguranju učinkovite zaštite zračnog prometa od suvremenih kibernetičkih izazova. Uslijed upita vezanih uz osiguravanje u zračnom prometu, ICAO je donio rezoluciju A39-19* koja precizira akcije i mjere za suprotstavljanje kibernetičkim napadima, obuhvaćajući ne samo države članice, već i druge relevantne strane (Čokorilo, 2020). U proteklom razdoblju koncept zaštite zračnog prometa na europskoj razini izmijenjen je i unaprijeđen, naravno sa odgovarajućim prilagodbama i izmjenama sustava na nacionalnoj razini. Izmjene i unaprjeđenja temelje se na odgovarajućim izmjenama europskog i nacionalnog zakonodavstva (Nađ, 2014).

ICAO, globalni regulator civilnog zrakoplovstva, nije jedini entitet koji oblikuje zakonodavni okvir kibernetičke zaštite u civilnom zrakoplovstvu. Europska Unija (EU) i pojedine države članice EU također dijele odgovornost u tom području. Suradnja između ICAO-a, EU i njenih članica ključna je za usklađivanje normativnih okvira na globalnoj i regionalnoj razini, osiguravajući konzistentnu i učinkovitu zaštitu od kibernetičkih prijetnji u zračnom prometu. Ovi entiteti igraju ključnu ulogu u ostvarivanju sigurnosti

---

* *International Civil Aviation Organization*

* *Annex 17: Aviation Security. Više na: https://www.icao.int/security/sfp/pages/annex17.aspx*

* *Više na: https://www.icao.int/aviationcybersecurity/Documents/A39-19.pdf*

zračnog prometa u informacijskom okruženju, a njihova suradnja presudna je za održavanje integriteta i pouzdanosti sustava upravljanja zračnim prometom.

U prosincu 2020. godine Europska komisija i Europska služba za vanjsko djelovanje (ESVD) predstavile su novu strategiju EU-a za kibersigurnost[*]. U sklopu tih napora, ENISA (Agencija Europske unije za kibersigurnost) pruža podršku državama članicama, institucijama EU-a i organizacijama, uključujući implementaciju Direktive o sigurnosti mrežnih i informacijskih sustava (NIS)[*]. Prijedlogom uredbe o kibersigurnosnim zahtjevima za proizvode s digitalnim elementima, poznatim kao Akt o kiberotpornosti[*] nastoji se ojačati sigurnosna pravila s ciljem osiguranja hardverskih i softverskih proizvoda. Međunarodni propisi i europski pravilnici postavljaju temeljne smjernice za zaštitu od kibernetičkih prijetnji, potičući svaku zemlju na nacionalnoj razini na implementaciju odgovarajućih mjera. Cilj je osigurati da zakoni i propisi na nacionalnoj razini budu usklađeni s najnovijim standardima kibernetičke sigurnosti, čime se stvara ujednačeni okvir podrške za kolektivnu zaštitu od kibernetičkih prijetnji. Implementacija međunarodnih propisa i pravilnika EU-a uključuje stvaranje i jačanje nacionalnih strategija kibernetičke sigurnosti, uspostavu tijela ili agencija odgovornih za praćenje provedbe, te donošenje zakona i propisa na nacionalnoj razini. Postojanje snažnog normativnog okvira ključno je za osiguranje od kibernetičkih rizika u upravljanju zračnim prometom. Precizno definirane smjernice i standardi u okviru normativnog sustava pružaju temelj za usklađivanje s najvišim standardima sigurnosti. Ovaj pristup ne samo da omogućuje učinkovitu prevenciju kibernetičkih prijetnji, već stvara i osnovu za brzu i koordiniranu reakciju u slučaju identificirane prijetnje.

6. ZAKLJUČAK

Analiza kibernetičkih prijetnji u sustavu upravljanja zračnim prometom ističe složenost i ozbiljnost izazova suvremenog civilnog zrakoplovstva. Unatoč prednostima razvoja visoko sofisticiranih informacijskih tehnologija

[*] *Više na: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy*

[*] *Direktiva (EU) 2022/2555 Europskog parlamenta i vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive 2016/1148 (Direktiva NIS 2).*

[*] *Više na: https://digital-strategy.ec.europa.eu/hr/policies/cyber-resilience-act*

za sigurnost i učinkovitost zračnog prometa, otvaraju se vrata raznolikim prijetnjama i rizicima.

Značajno je uočiti sve češće pojavljivanje kibernetičkih napada na sustave upravljanja zračnim prometom, s njihovim potencijalno značajnim utjecajem na sigurnost. Ovaj rad postavlja temelje za daljnji razvoj i implementaciju sigurnosnih mjera kroz detaljnu analizu metodologija procjene rizika, normativnih okvira te ključnih aspekata kibernetičke sigurnosti.

S obzirom na sveprisutnu digitalizaciju i povezanost zračne plovidbe, naglašava se potreba za stalnim unaprjeđenjem i prilagodbama sustava upravljanja zračnim prometom. Ključno je budućnosti posvetiti pažnju kontinuiranom unaprjeđenju sigurnosnih mjera, posebno u dinamičnom okruženju kibernetičkih prijetnji. Suradnja između različitih sudionika u zračnom prometu postaje presudna, jer razmjena informacija o prijetnjama i najboljim praksama doprinosi jačanju općeg sustava sigurnosti. Edukacija i osvještavanje zaposlenika ključni su čimbenici u odgovoru na kibernetičke prijetnje, s posebnim naglaskom na svijest o rizicima i sposobnostima pravovremene reakcije na potencijalne prijetnje.

U budućnosti, nužno je pratiti stalno evoluirajuće prijetnje te prilagoditi sigurnosne strategije kako bi se održala integritet i sigurnost sustava upravljanja zračnim prometom. To uključuje kontinuirano ulaganje u sigurnosna rješenja, poticanje suradnje među dionicima, inventivno obrazovanje, praćenje tehnoloških inovacija te brzu i učinkovitu reakciju na identificirane prijetnje.

LITERATURA

1. Ahić, J., Nađ, I., 2017. Upravljanje rizikom u privatnoj sigurnosti. Sarajevo: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije.
2. CANSO Cybersecurity Risk Assessment Guide, 2023. Civil Air Navigation Services Organisation. [online] Dostupno na: https://canso.fra1.digitaloceanspaces.com/uploads/2023/05/CANSO-Safety_Cybersecurity-Risk-Assessment-Guide-2023.pdf.
3. Cybersecurity Culture in Civil Aviation. (2022). International Civil Aviation Organization (ICAO). [online] Dostupno na: https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Culture%20in%20Civil%20Aviation.EN.pdf
4. Čokorilo, O., 2020. Bezbednost vazduhoplova (II dopunjeno izdanje). Beograd: Saobraćajni fakultet.
5. Guidelines for the Oversight of Air Traffic Management Security, 2022. EUROCONTROL. [online] Dostupno na: https://www.eurocontrol.int/publication/eurocontrol-guidelines-oversight-air-traffic-management-security
6. Masleša, R., 2001. Teorije i sistemi sigurnosti. Sarajevo: Magistrat
7. Nađ, I., 2014. Zaštitni pregled putnika i prtljage od strane privatne zaštite na zračnim lukama. Kriminalistička teorija i praksa. 1 (1), str. 81-95.
8. Obradović, D., 2018. Kibernetika – što je to?. Common Foundations 2018 - uniSTem: 6th Congress of Young Researchers in the Field of Civil Engineering and Related Sciences. Split: Sveučilište u Splitu, Fakultet građevinarstva, arhitekture i geodezije. str. 158-163.
9. Pavlin, S., 2006. Aerodromi 1. Zagreb: Fakultet prometnih znanosti.
10. Steiner, S., 1998. Elementi sigurnosti zračnog prometa. Zagreb: Fakultet prometnih znanosti.
11. Direkcija za civilno zrakoplovstvo Bosne i Hercegovine (BHDCA), 2014. Uputstvo o upravljanju rizicima u sistemu sigurnosti letenja. [online] Dostupno na: http://www.bhdca.gov.ba/website/dokumenti/Bezbjednost_letenja/UPUTSTVO_rizici_bos.pdf