

UPORABA UMETNE INTELIGENCE IN KIBERNETSKA VARNOST NA LETALIŠČIH

mag. Robert Rauch, Fraport Slovenija, d.o.o.

Izvleček

Tehnološke izboljšave na osnovi inovativnih tehnologij, kot je umetna inteligenca, ki bodo trajnostno naravnane, imajo velik potencial. V kontekstu dolgoročne rasti letalskih potovanj, stalnih stroškovnih pritiskov na letališčih in hitrega napredka inovativnih tehnologij se odpirajo številne priložnosti. Hkrati pa uporaba tovrstnih tehnologij na letališčih s seboj prinaša tudi pomisleke o informacijski varnosti in zasebnosti, ki jih je treba nasloviti z ustrezno zakonodajo, regulacijo, etičnimi smernicami in varnostnimi protokoli. Letališča tako ne smejo zanemariti kibernetске varnosti, ki posledično postaja vse večji izziv. V prispevku bomo analizirali nekaj najboljših praks.

Ključne besede: letališča, sodobne tehnologije, umetna inteligenca, kibernetška varnost

USE OF ARTIFICIAL INTELLIGENCE AND CYBERSECURITY IN AIRPORTS

Abstract

Technological improvements based on innovative technologies, such as artificial intelligence, which are sustainability-oriented, have great potential. In the context of long-term growth in air travel, constant cost pressures on airports, and the rapid advancement of innovative technologies, numerous opportunities are emerging. However, the use of such technologies at airports also raises concerns about information security and privacy, which must be addressed through appropriate legislation, regulation, ethical guidelines, and security protocols. Therefore,

airports must not neglect cybersecurity, which is becoming an increasingly significant challenge. In this paper, we will analyze some of the best practices.

Key words: airports, modern technologies, artificial intelligence, cyber security

1 UVOD

Letališča se spopadajo s številnimi izzivi, zato iščejo rešitve z vpeljanjem novih tehnologij, ki temeljijo na digitalizaciji in avtomatizaciji operativnih postopkov. V kontekstu dolgoročne rasti letalskih potovanj, stalnih stroškovnih pritiskov in hitrega napredka inovativnih tehnologij na letališčih se odpirajo številne priložnosti. Tehnološke izboljšave na osnovi inovativnih tehnologij, kot je umetna inteligenca, imajo velik potencial (Mitchel, 2020; Davenport, 2019 in Norman, 2024). Vprašanj o prihodnosti je več, kot je na voljo odgovorov. Zato je bistvenega pomena razumevanje vpliva tovrstnih tehnologij na letališča, ki so pod stalnim pritiskom zmanjšanja stroškov in izboljšanja operativne učinkovitosti (Rauch, 2022).

Avtomatizacija in digitalizacija s seboj prinašata tudi številne izzive in tveganja glede kibernetске varnosti (IATA, 2019). Koncept pametnih letališč (ang. *Smart Airports*), ki temelji na optimizaciji operativne učinkovitosti, s seboj prinaša tudi številne izzive (Rauch, 2017). V samo nekaj letih smo se soočili s povsem novimi vrstami groženj. Tudi umetna inteligenca je v medijih pogosto izpostavljena v negativni luči z napovedmi ukinjanja delovnih mest, poseganja v človeške pravice, plagiatstvo ... Daleč od tega, da bi to bili le namišljeni problemi (Živec, 2023). Za celovit vpogled ter razumevanje njenih prednosti in slabosti moramo najprej vedeti, kaj umetna inteligenca sploh je in kako nam lahko pomaga.

2 UMETNA INTELIGENCA

Umetno inteligenco (ang. *Artificial Intelligence* – AI) umeščamo v področje računalništva in informatike, ki se ukvarja z razvojem sistemov za izvajanje nalog, ki običajno zahtevajo človeško inteligenco, kot so zaznavanje, razmišljanje, učenje in reševanje problemov (Živec, 2023).

AI, opisana kot sposobnost prilagajanja spremembam (Hawking in Murray, 2022), se je razvijala od 50. let prejšnjega stoletja, ko je John McCarthy prvič skoval izraz umetna inteligenca (Brynjolfsson in McAfee, 2019).

Danes večina AI deluje na ravni »osnovne AI«, ki temelji na podatkih in predpostavkah ter je zelo učinkovita pri specifičnih nalogah. Ključna tehnologija za to je strojno učenje (ang. *Machine Learning* – ML), ki računalnikom omogoča učenje iz podatkov in izboljšanje delovanja. Strojno učenje je uporabno pri prepoznavanju vzorcev, klasifikaciji in napovedovanju. Naprednejše tehnologije vključujejo nevronske mreže, globoko učenje in naravno jezikovno procesiranje (Mitchel, 2020 in Davenport, 2019). Končni cilj predstavlja „napredna AI“, ki bi bila sposobna razmišljati in se zavesti kot ljudje.

Uporaba AI je razširjena v industriji, medicini, financah in drugih sektorjih, kjer izboljšuje učinkovitost in odločanje. Tudi v zasebnem življenju smo že redni uporabniki AI, z orodji kot je ChatGPT, ki odgovore podaja v nekaj sekundah. Ključno pa je izbrati pravo rešitev ob upoštevanju zasebnosti, zaupnosti in varnosti (Djurđič, 2024).

2.1 Umetna inteligenca in moč podatkov

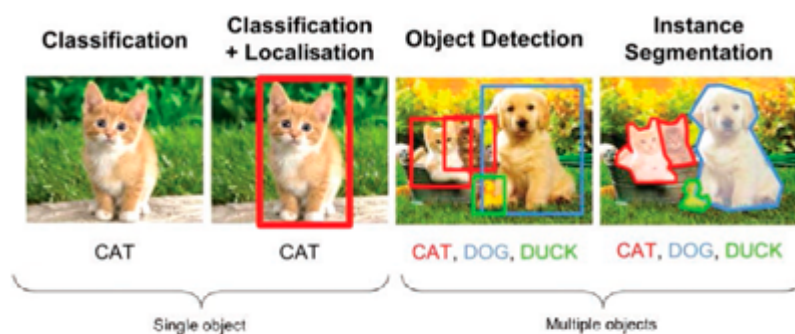
Digitalizacija in avtomatizacija procesov lahko vpliva na učinkovitost in produktivnost ter ob podpori podatkov izboljša in pospeši sprejemanje odločitev. Optimizacija

operativnih procesov, ki temelji na analizi večjih količin strukturiranih podatkov, ni novost (strukturirani podatki so podatki, ki jih je mogoče logično organizirati v vrsticah in stolpcih). Šele nedavno pa je zaradi prebojev na področjih AI in naprednega računalništva mogoče analizirati tudi nestrukturirane podatke, kot so zvok, video in fotografije (Hen, 2023). Tehnologija računalniškega vida, ki se uporablja za zaznavanje predmetov, je prikazana na sliki 1.

2.2 Pomisleki glede umetne inteligence

Številni znanstveniki, vključno s Hawkingom in Murrayem (2022), opozarjajo, da bi AI lahko predstavljala eksistencialno grožnjo. Kirsch (2024) primerja njen potencial z jedrsko bombo. Hopfield in Hinton, Nobelova nagrajenca za fiziko 2024, menita, da je brez nadzora lahko nevarna, in poudarjata nujnost razumevanja tehnologije (STA, 2024). Plenty in Morrissey (2019) pa ugotavljata, da je tehnologija sama po sebi nevtralna – ključno je, kako jo uporabljamo.

Uporaba tehnologij na osnovi AI hkrati s seboj prinaša pomisleke tudi o informacijski varnosti in zasebnosti (zloraba osebnih podatkov, nadzor ipd.), ki jih je treba reševati z ustrezno regulacijo in spoštovanjem zakonodaje. Pomembno je, da se uporaba umetne inteligence (na letališčih) izvaja odgovorno, etično in ob upoštevanju varstva zasebnosti ter pravic potnikov.



Slika 1: Tehnologija računalniškega vida, ki se uporablja za zaznavanje predmetov. (Vir: Hen, 2023)

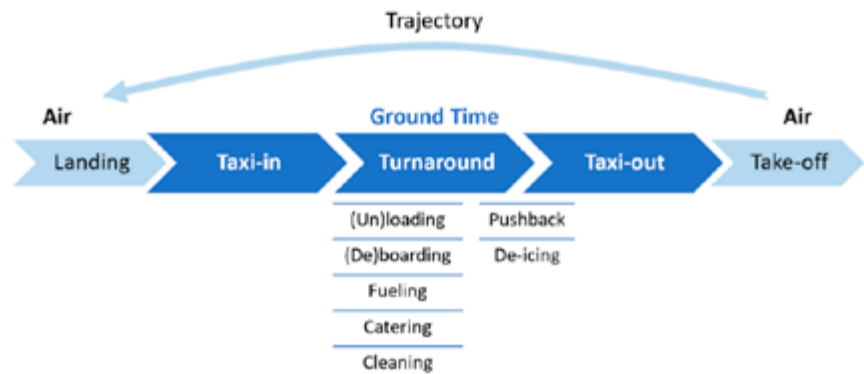
2.3 Prisotnost umetne inteligence na letališčih

AI je na letališčih že nekaj časa prisotna in uveljavljena na kar nekaj področjih (Davenport, 2019). V ugledni letalski reviji *Passenger Terminal World* so predstavljeni najnovejši primeri uporabe AI na letališčih. Po podatkih Microsoftovega oddelka za letalstvo v Združenem kraljestvu naj bi AI korenito spremenila delovanje letališč po vsem svetu (Norman, 2024). Na trgu že obstajajo rešitve, kot so na primer avtomatizirane objave, ki lahko s pomočjo umetne inteligence samodejno prevajajo besedila in govor med različnimi jeziki (Aviavox, 2023). Letališča lahko s pomočjo AI znatno izboljšajo na primer energetske upravljanje, kar prispeva k zmanjšanju izpustov toplogrednih plinov in podpira trajnostni razvoj.

3 PRIMER PRAKTIČNE UPORABE UMETNE INTELIGENCE PRI OPTIMIZACIJI ZEMELJSKE OSKRBE LETAL NA LETALIŠČU LJUBLJANA

3.1 Zamude pri obračanju letal

Zamuda letala na tleh (ang. *Ground Delay*) se nanaša na čas, ko je letalo zadržano pred vzletom ali po pristanku. Do zamud lahko pride zaradi omejitev v zračnem prostoru, vremenskih razmer ali operativ-



Slika 2: Obračanje letala. (Vir: Hutter in Pfennig, 2023)

nih razlogov. Te zamude vplivajo na učinkovitost letalskih operacij, povzročajo dodatne zamude, višje stroške ter nezadovoljstvo potnikov. Zmanjševanje teh zamud je ključno za ohranjanje učinkovitosti in zanesljivosti letalskega prometa. Pri analizi zamud letal na letališču iz operativnih razlogov smo na letališču Ljubljana želeli pridobiti globlji pogled v tovrstno problematiko. Splošni proces obračanja letala na letališču je prikazan na sliki 2.

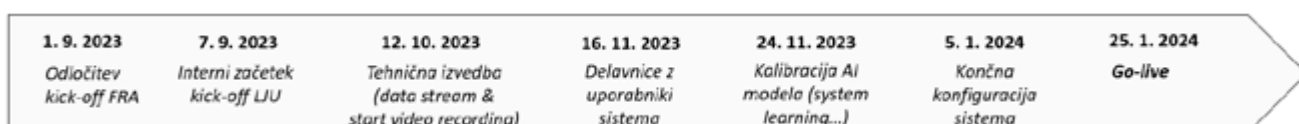
Ključni izziv je razumevanje trajanja posamezne aktivnosti pri obračanju letal oziroma prepoznavanje pomanjkljivosti, s ciljem izboljšati učinkovitost ter zmanjšati zamude letal.

3.2 Proaktivno AI orodje (Apron AI)

Najnovejša tehnologija na letališčih vključuje orodja za nadzor obračanja letal (ang. *Turnaround process*), ki temeljijo na naprednem računalništvu in AI. Namen je izboljšati

operativno učinkovitost, varnost, zmanjšati zamude ter spodbujati trajnostni razvoj. Nekatera letališča že dosegajo odlične rezultate pri zmanjševanju čakalnih vrst, kar zmanjšuje porabo goriva, operativne stroške in emisije CO₂ (Hen, 2023). Proaktivno AI orodje (Apron AI) s kombinacijo računalniškega vida in umetne inteligence samodejno spremlja vse aktivnosti pri obračanju letal ter omogoča predvidljivost zaključka postopkov. Letališče Ljubljana je kot eno izmed prvih v Evropi uvedlo to tehnologijo v začetku leta 2024 (Rauch, 2023), projekt pa je bil zaključen v rekordnih štirih mesecih (glej sliko 3).

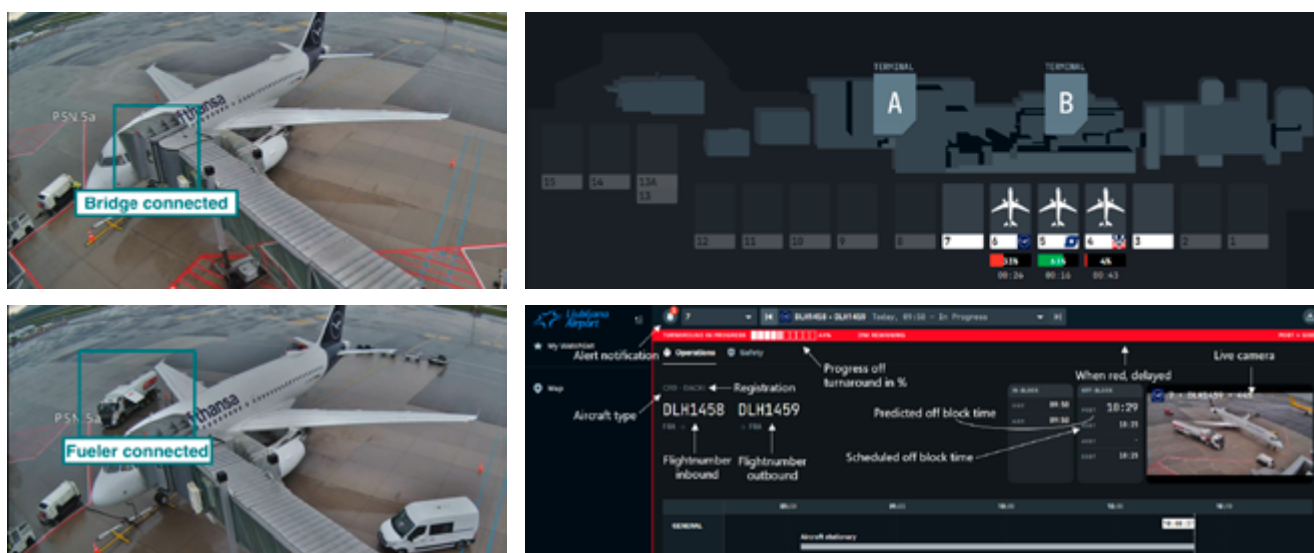
Projektna ekipa je najprej analizirala in ocenila primernost izbranih lokacij kamer za pokrivanje operativnih aktivnosti, varnostnih vidikov, uporabe opreme itd. Optimalno pokritost posameznega parkirnega mesta zagotavljata (že) dve nameščeni kameri (slika 4).



Slika 3: Časovnica izvedbe projekta na letališču Ljubljana (Vir: Fraport Slovenija, 2024)



Slika 4: Namestitev kamer na letališču Ljubljana. (Vir: Fraport Slovenija, 2024)



Slika 5: Nadzorna plošča. (Vir: Fraport Slovenija in Assaia, 2024)

Orodje ima možnost samodejnega generiranja časovnih žigov (ang. *Time Stamps*), ki označujejo začetek in konec procesnih aktivnosti, kot so nalaganje prtljage, polnjenje goriva, vkrcavanje potnikov itd. Gre za kompleksen sistem napovednih sposobnosti. Napovedna natančnost se z vsakim obratom letala izboljšuje in že dosega izjemne ravni. Temelji na algoritmih strojnega učenja za analizo podatkov v realnem času. Proaktivno AI orodje ponuja vpogled v realnem času prek uporabniku prijaznega grafičnega vmesnika (slika 6).

Sistem je nameščen na vseh ključnih izhodih (ang. *Gates*) oziroma aviomostovih, kar nam omogoča, da v realnem času optimiziramo operativne postopke, vključno z dodeljevanjem optimalnega števila osebja glede na dejanske dogodke. Ključni vpogledi na nadzorni plošči vključujejo dejanske in historične podatke, vključno z video sliko. Pridobljeni podatki so integrirani v ostale informacijske sisteme letališča in zagotavljajo vse potrebne informacije. Vključujejo tudi prilagojena opozorila, ki obveščajo o morebitnih težavah ali zamudah, ter podrobna prilagojena poročila, ki so podlaga za dolgoročne izboljšave (slika 6).



Slika 6: Prilagojena poročila. (Vir: Fraport Slovenija in Assaia, 2024)

3.3 Ključni rezultati

Cilj je bil z inovativnimi rešitvami optimizirati operativne postopke, kar vodi v manj zamud, večjo varnost in trajnostni razvoj. Z orodjem Apron AI lahko hitro prepoznamo operativne izzive in izboljšamo učinkovitost procesov, kar omogoča boljšo integracijo umetne inteligence z operativnim osebjem. S sprotnimi informacijami v realnem času osebje hitro prepozna ozka grla, lahko prerazporedi vire in poveča operativno učinkovitost. Prvi rezultati kažejo na opazno zmanjšanje povprečnih zamud zaradi poznih prihodov letal za skoraj šest minut.

4 KIBERNETSKA VARNOST V LETALSKEM PROMETU

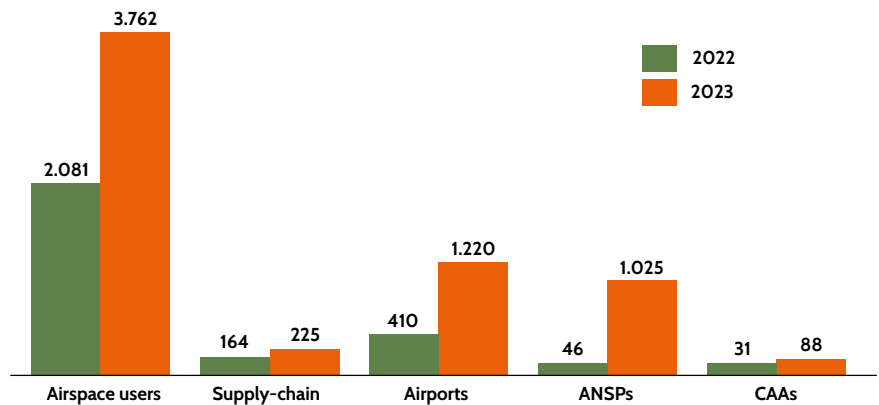
4.1 Osnove kibernetске varnosti

Kibernetško varnost lahko opredelimo kot zbirko orodij, politik, varnostnih konceptov, varnostnih ukrepov, smernic, pristopov za obvladovanje tveganj, usposabljanja, najboljših praks, jamstev in tehnologij, ki jih lahko uporabimo za zaščito kibernetškega okolja ter premoženja organizacij in uporabnikov (IATA, 2019). Enotne definicije tega pojma sicer ni, po nekaterih opredelitvah naj bi kibernetška varnost vključevala ne le zaščito pred namernimi napadi, ampak tudi npr. zaščito opreme v primeru naravnih

nesreč. Zato je kibernetska varnost širši pojem od spletne varnosti oz. internetne varnosti (Čičerov, 2024).

4.2 Kibernetske grožnje in napadi v letalskem prometu

Civilno letalstvo je privlačna tarča za kibernetske napade (ICAO, 2018). Evropska agencija za varnost v letalstvu (European Union Aviation Safety Agency - EASA) je uvedla vrsto pobud za izboljšanje obvladovanja kibernetskih tveganj v letalstvu ter ustvarjanje okolja, v katerem je Evropska unija bolje pripravljena učinkovito obravnavati tovrstna tveganja. Ena od glavnih prednostnih nalog EASA je doseči kibernetsko odporno letalstvo (EASA, 2017). Po podatkih Eurocontrola (2024) se vsako leto povečuje število napadov na letalsko IT infrastrukturo. Ponudnik tehnoloških rešitev v zračnem prometu SITA (2017) meni, da je sposobnost hitrega in učinkovitega odziva na kibernetske grožnje ključnega pomena. Porazdelitev napadov, ki jih je zaznal Eurocontrol v letih 2022 in 2023, kaže na precejšnje razlike med letalskimi deležniki. Največji odstotek napadov beležijo letalski prevozniki (slika 7).



Slika 7: Kibernetski napadi: primerjava v letih 2022 in 2023. (Vir: Eurocontrol, 2024)

Kibernetski napadi v letalstvu poleg varnostnih tveganj povzročajo tudi pravne in finančne posledice, da ne govorimo o izgubi ugleda. Po podatkih Agencije EU za kibernetsko varnost (ENISA, 2024) je mesečno ukradenih več kot 10 terabajtov podatkov. Izsiljevalska programska oprema (ang. *ransomware*) predstavlja eno od največjih groženj, medtem ko je spletno ribarjenje (ang. *phishing*) najpogostejši vektor napadov. Kibernetske grožnje vključujejo tudi zlonamerno programsko opremo (ang. *malware*). Stroški kibernetske kriminalitete so dosegli 5,5 milijona EUR letno, kar je dvakrat več kot leta 2015 (ENISA, 2024).

Nekaj zadnjih primerov. Julija 2024 je izsiljevalska združba Akira ohromila IT-infrastrukturo splitskega letališča, kar je povzročilo številne odpovedi letov (HRT, 2024). Incident se je zgodil le nekaj dni po globalnem izpadu informacijskih sistemov, po posodobitvi antivirusne programske opreme CrowdStrike, ki je prizadela številna podjetja, tudi banke, vključno z ljubljanskim letališčem, kjer so nastale manjše zamude (RTV, 2024). Avgusta 2024 je napad na letališče Seattle-Tacoma onemogočil sisteme za prikaz letov in povzročil odpovedi (Airport International Review, 2024). Nekaj izstopajočih primerov kibernetskih napadov v zadnjih letih v svetu je



Leto	Organizacija	Vrsta incidenta	Podrobnosti vpliva
2024	Letališče Seattle	Zlonamerna koda (malware)	Izpad letališkega informacijskega sistema (FIDS); onemogočen Wi-Fi; več kot 400 zamud in odpovedanih letov; zaustavitev sistema za prtljago.
2024	Letališče Split	Izsiljevalski napad (ransomware)	Številni odpovedani leti in zamude; podatki podrobnosti napada niso na voljo.
2023	Air France	Ribarjenje (phishing)	Dostop do podatkov potnikov in zaposlenih; - Prizadetih več kot 10 milijonov ljudi.
2022	Ruska zvezna agencija za zračni promet	Izsiljevalski napad (ransomware)	Anonymous Hacking Group; izbris 65 TB podatkov (registracije letal, e-pošte, varnostne kopije); neučinkovit sistem varnostnih kopij.
2022	Sunwing	Izsiljevalski napad (ransomware)	Velike zamude/odpovedi letov zaradi okužbe IT.
2021	SITA (ponudnik tehnoloških rešitev)	Ribarjenje (phishing)	Oskrbuje 90 % svetovnih letalskih družb; prizadetih 11 prevoznikov in 2,1M potnikov.
2019	Air New Zealand	Ribarjenje (phishing)	Dostop do programa zvestobe (120.000 članov)
2018	Cathay Pacific	Kraja podatkov	Prizadetih 9,4M računov potnikov; pomanjkanje zaščite gesel.
2018	British Airways	Zlonamerna koda (malware)	Ukradeni osebni podatki 429.612 oseb in podatki 244.000 kreditnih kartic.

Tabela 1: Nekaj izstopajočih primerov kibernetских napadov po svetu. (Vir: HRT, 2024; Airport Technology, 2024 in Mencinger, 2024)

prikazanih v tabeli 1, kjer so navedene tudi ključne podrobnosti posameznega incidenta.

4.3 Izzivi kibernetске varnosti in strategije obvladovanja tveganj na letališčih

Kibernetске grožnje se hitro množijo in postajajo vse bolj kompleksne (ACRP, 2015). Kljub napredku tehnologij številni napadi izhajajo iz osnovnih ranljivosti, povezanih s človeškimi napakami, kot so slabo ravnanje z gesli, klikanje na sumljive povezave in izpostavljanje občutljivih informacij. Obvladovanje tveganj vključuje redno menjavo gesel, večstopenjsko avtentikacijo, šifriranje podatkov, antivirusno zaščito in redna posodabljanja programske opreme. Ključno pa je usposabljanje in ozaveščanje zaposlenih (Gotlieb, 2016).

varnosti in zasebnosti, kot so na primer zloraba osebnih podatkov, nadzorovanje posameznikov na letališčih, možnost zlorabe tehnologije za nezakonite namene, napake prepoznavanja, pravice dostopa do podatkov in kako so ti podatki shranjeni in varovani itd. (Davenport, 2019).

Vse te pomisleke je treba nasloviti z ustrežno zakonodajo, regulacijo, etičnimi smernicami in varnostnimi protokoli (Hen, 2023). Treba je najti ravnotežje med uporabo tehnologij AI za izboljšanje varnosti in storitev ter zagotavljanjem varstva zasebnosti in pravic posameznikov. Letališča tako nikakor ne smejo zanemariti kibernetске varnosti (Rau- ch, 2019), ki postaja vse večji izziv in bi lahko ogrozili tudi sisteme AI, kar zahteva sodelovanje med vsemi vpletenimi deležniki.

nost ščiti sisteme in omrežja pred digitalnimi napadi. AI ni le intelektualna modna muha, temveč že pomembno vpliva na naš vsakdan, čeprav se tega pogosto ne zavedamo (Živec, 2023 in Djurdjić, 2024). Ob tem je razumevanje in zmanjševanje kibernetских tveganj in človeškega faktorja pomembnejše kot kdajkoli prej. Digitalna transformacija z AI pogosto ne spodleti zaradi tehničnih izzivov, ampak zaradi „kulturnega odpora“.

V prihodnosti bo AI igral vedno večjo vlogo v letalski industriji, kar bo izboljšalo učinkovitost in trajnost sektorja, vendar pa povečana uporaba AI prinaša tudi večjo izpostavljenost kibernetским tveganjem. Letalska industrija je zaradi svoje izpostavljenosti še posebej privlačna tarča kibernetских napadov, zato je nujno nenehno nadgrajevanje varnostnih ukrepov ter zagotavljanje zaščite podatkov in sistemov.

5 PRIHODNOST UMETNE INTELIGENCE IN KIBERNETSKЕ VARNOSTI

Prihodnost AI in kibernetске varnosti je polna priložnosti in izzivov. Uporaba tehnologij na osnovi AI na letališčih s seboj prinaša kar nekaj pomislekov o informacijski

6 ZAKLJUČEK

Umetna inteligenca (AI) in kibernetска varnost sta temeljna gradnika sodobnega digitalnega sveta. AI omogoča računalnikom učenje iz izkušenj ter opravljanje nalog, ki običajno zahtevajo človeško inteligenco, medtem ko kibernetска var-

Mag. Robert Rauch, Fraport Slovenija je izkušen strokovnjak s področja letalskega prometa. Na letališču Ljubljana, ki ga upravlja Fraport Slovenija, je s svojo ekipo sodeloval pri številnih projektih, tudi kot izvršni vodja projekta razširitve potniškega terminala. V zadnjih letih je zadalžen za vpeljavo novih tehnologij ter inovacijske projekte.

LITERATURA IN VIRI

ACRP (Airport Cooperative Research Program). 2015. Report 140: Guidebook on Best Practices for Airport Security, TRB, 2015.

ACI (Airports Council International). 2017. Airport Digital Transformation – Best practice.

Airport International Review. 2024. Seattle-Tacoma International Airport still recovering from cyberattack. <https://www.internationalairportreview.com/news/226474/sea-airport-still-recovering-from-cyberattack/> (pridobljeno 12. 9. 2024).

Assaia. 2024. Apron AI. www.assaia.com/solutions/apron-ai (pridobljeno 10. 5. 2024).

Aviavox. 2024. Intelligent Artificial Voice Systems. www.aviavox.com (pridobljeno 12. 5. 2024).

Brynjolfsson, E., McAfee, A. 2019. The Business of Artificial Intelligence. Harvard Business Review Press, Boston, Massachusetts.

Čičerov, P. Letalske organizacije in kibernetika varnost. 2024. Konferenca o letalski varnosti (21–22. 05. 2024, Laško). Javna agencija za civilno letalstvo.

Davenport, T. H., (2019), Artificial Intelligence, Harvard Business Review Press, Boston, Massachusetts.

Djurdjić, V. 2024. Oblačna in lokalna inteligenca. Revija Monitor, maj 2024.

EASA (European Union Aviation Safety Agency). 2024. Cybersecurity Overview. www.easa.europa.eu/ (pridobljeno 5. 9. 2024).

ENISA (Agencija EU za kibernetiko varnost). 2024. Glavne kibernetične grožnje v EU. www.consilium.europa.eu/si/infographics/cyber-threats-eu/ (pridobljeno 11. 9. 2024).

Eurocontrol. 2024. European Air Traffic Management. Computer Emergency Response Team. Report on Cyber in Aviation.

Fraport Slovenija. 2024. Interno gradivo.

Gotlieb, J. 2016. Cybersecurity. Passenger Terminal World. June 2016.

Hawking, S., Murray, J. 2022. Will Artificial Intelligence Outsmart Us? J. Murray Publishers.

Hen, C. 2023. Airport Management: You cannot manage what you cannot measure. Journal of Airport Management, Vol 17. No3. 278–290 Summer 2023.

HRT. 2024. Split airport after the hacker attack: We will not negotiate. <https://glashrvatske.hrt.hr/en/domestic/split-airport-after-the-hacker-attack-we-will-not-negotiate-11673909> (pridobljeno 5. 9. 2024).

Hutter, F.G, Pfennig, A. 2023. Reduction in Ground Times in Passenger Air Transport: A First Approach to Evaluate Mechanisms and Challenges. Applied Sciences. 2023, 13, 1380. <https://doi.org/10.3390/app13031380>. <https://www.mdpi.com/journal/applsci> (pridobljeno 11. 5. 2024).

IATA (International Air Transport Association). 2019. Cyber Security.

ICAO (International Civil Aviation Organization). 2018. Airport Preparedness on cyber resilience, ICAO Working paper. Montreal. October 2018. (www.icao.int).

Kirsch, A. 2024. Najpametnejši človek, ki jih je kdaj živel. The Atlantic. Povzeto v Reviji Monitor Svet. april 2024.

Mencinger, M. 2024 Kibernetika v letalstvu. Konferenca o letalski varnosti (21–22. 5. 2024, Laško). Javna agencija za civilno letalstvo.

Mitchel, M. 2020. Artificial Intelligence – A guide for Thinking Humans. Pelican Penguin Books.

Norman, H. 2024. Artificial Intelligence. Passenger Terminal World, January 2024.

Plenty, R., Morrissey T. 2019. Utopia or dystopia? People matters. Airport World, Issue 5. 2019.

SITA (Société Internationale de Télécommunications Aéronautiques), Cybersecurity Aviation. SOC, 2017.

Rauch, R. 2017. Smart Airports. Automation in transportation 2017, Korema, Avtomatizacija u prometu, Zbornik radova (str. 82–89). Rijeka, Croatia.

Rauch, R. 2019. Cyber security in aviation, the airports perspective. Automation in transportation 2019, Korema, Avtomatizacija u prometu 2019, Zbornik radova (str. 6–9). Split, Croatia.

Rauch, R. 2022. Vpliv digitalizacije na razvoj potniških terminalov. Izzivi trajnostnega razvoja: zbornik konference (str. 96–106). B&B Visoka šola za trajnostni razvoj.

Rauch, R. 2023. Sodobne tehnologije in umetna inteligenca: Vplivi na letališča. Izzivi trajnostnega razvoja: zbornik konference (str. 24–31). B&B Visoka šola za trajnostni razvoj.

RTVSLO. 2024. Prizadeta podjetja zaradi izpadov informacijskih sistemov so iz zelo različnih sektorjev. www.rtvsi.si/znanost-in-tehnologija/svete-prizadeta-podjetja-zaradi-izpadov-informacijskih-sistemov-so-iz-zelo-razlicnih-sektorjev/715409 (pridobljeno 9. 9. 2024).

STA. 2024. Nobelova nagrada za fiziko svarita pred nevarnostmi umetne inteligence. www.sta.si/3350828/nobelova-nagrada-za-fiziko-svarita-pred-nevarnostmi-umetne-inteligence (pridobljeno 10. 10. 2024).

Živec, R. 2023. Prednosti in pasti umetne inteligence. Glas gospodarsva, marec 2023.