HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 2. szám 123–148.
DOI: 10.32567/hm.2024.2.10

Katona Gergő[1]

Kiberbiztonsági stratégiák, szabályozások és ajánlások az okosrepülőterek számára: fenyegetések és megoldások

Cybersecurity Strategies, Regulations and Recommendations for Smart Airports: Threats and Solutions

Absztrakt

Az okosrepülőterek digitális és hálózati integrációja miatt a kiberbiztonság kulcsfontosságú. A repülőtéri folyamatok digitalizálása, az automatizálás és a személyre szabott utasélmény iránti igény új kiberbiztonsági kihívásokat teremt. Az USA, az EU és nemzetközi légi közlekedési szervezetek jogszabályokkal és ajánlásokkal segítik a repülőterek információbiztonsági szintjének növelését, hogy jobban ellenálljanak a kibertámadásoknak. A kutatás célja, hogy azonosítsa az okosrepülőterek specifikus rendszerelemeit és az ezekre leselkedő kiberbiztonsági fenyegetéseket. Nemzetközi dokumentumok elemzésével a cikk feltérképezi, az Európai Unió, az Egyesült Államok és nemzetközi légi közlekedési szervezetek által közzétett, a szektorral kapcsolatos publikációk milyen mélységgel foglalkoznak a kiberbiztonsággal, illetve milyen szinten adnak választ az azonosított fenyegetésekre. A kutatás eredményei hozzá tudnak járulni az okosrepülőterek biztonsági szintjének javításához és a kiberfenyegetésekkel szembeni védelemük megerősítéséhez.

Kulcsszavak: okosrepülőtér, kiberbiztonság, IoT, érettség, Alverad

[1] Junior kutató, Nemzeti Közszolgálati Egyetem, e-mail: katona.gergo@uni-nke.hu

Abstract

With the digital and network integration of smart airports, cyber security is key. The digitalisation of airport processes, automation and the need for a personalised passenger experience are creating new cyber security challenges. The US, the EU and international aviation organisations are helping airports improve information security through legislation and recommendations to make them more resilient to cyberattacks. The aim of this research is to identify the specific system components of smart airports and the cybersecurity threats they face. Through an analysis of international documents, the article explores the depth to which publications published by the European Union, the United States and international aviation organisations on the sector address cybersecurity and the level of response to identified threats. The results of this research can contribute to improving the security level of smart airports and strengthening their defences against cyber threats.

Keywords: smart airport, cybersecurity, IoT, maturity, Alverad

Bevezetés

Az okosrepülőterek korszakában, ahol a digitális technológiák és a hálózatok kapcsolata határozza meg a működés minden aspektusát, a kiberbiztonság kérdése kiemelten fontos. Az egyes tényezők, mint például a repülőtéri folyamatok egyre nagyobb mértékű digitalizálódása és automatizálása, a személyre szabott utasélmény kialakításának igénye, valamint a légi közlekedés mint azonosított kritikus infrastruktúra ágazat jelentős kihívásokat rejt magában kiberbiztonsági területen. Az USA, az EU szervezetei, valamint a nemzetközi légi közlekedési szervezetek érzékelik a repülőterek és a légi közlekedés kiberbiztonsági kihívásait, ezért jogszabályokkal, ajánlásokkal és tervekkel segítik a szereplők információbiztonsági érettségi szintjének növelését. Az ilyen szabályozások és iránymutatások célja, hogy erősítsék a szervezetek ellenálló képességét a kibertérből jövő fenyegetésekkel szemben.

A tudományos probléma meghatározása

Az okosrepülőterek számos különböző típusú rendszerekből állnak, amelyek folyamatosan hatással vannak egymásra. A rendszerek egymástól való magas fokú függése az egyes rendszerelemek kiberbiztonsági sebezhetőségének értékét felerősítheti. Ezen sebezhetőségek kihasználása a légi közlekedésben hatalmas anyagi károkat tud okozni, és akár emberéleteket is veszélyeztet. Ezért fontos, hogy az ilyen típusú rendszerekkel rendelkező repülőterek rendszer-, fenyegetés- és követelménykörnyezetét azonosítsuk és kiértékeljük.

Módszertan

A kutatás során a szerző *state-of-art* analízissel vizsgálja meg, hogy milyen specifikus rendszerelemeket lehet azonosítani egy okosrepülőtér esetében, illetve ezek milyen kiberbiztonsági fenyegetéssel néznek szembe. Ezen nemzetközi dokumentumvizsgálattal térképezi fel a szerző azokat a szabályozásokat, irányelveket, stratégiákat, ajánlásokat, amelyekkel az egyes európai uniós vagy egyesült államokbeli, illetve nemzetközi légi közlekedési szervezetek publikáltak a légi közlekedés kiberbiztonságával kapcsolatban. Illetve a feltérképezett dokumentumokat csoportosítom az alapján, hogy milyen részletességgel vizsgálják a kiberbiztonságot. Azokat a dokumentumokat is elemzem, amelyekben a legrészletesebben fejtik ki a légi közlekedés kiberbiztonságát. A szerző azt vizsgálja, hogy az előzőleg azonosított fenyegetésekkel kapcsolatban milyen szintű segítséget tudnak nyújtani a dokumentumok.

Kutatási hipotézisek

A szerző a kutatás kezdetén az alábbi hipotéziseket fogalmazta meg:

H1: Az Egyesült Államok szervezetei több és részletesebb dokumentumot publikálnak a légi közlekedés kiberbiztonságával kapcsolatban, mint az Európai Unió intézményei.

H2: A nemzetközi módszertanok, dokumentumok implementálásával az azonosított kiberbiztonsági fenyegetések bekövetkezési kockázata csökkenthető az okosrepülőterek esetében.

A kutatás célkitűzése

A kutatás célja átfogó képet nyújtani az okosrepülőterek fogalmáról és az azt megalkotó rendszerekről. Azonosítani azokat a kihívásokat, amelyekkel szembe kell néznie az okosrepülőteret üzemeltetőnek. További célja a kutatásnak egy átfogó elemzés, amely megvizsgálja, hogy az Egyesült Államok, illetve az Európai Unió egyes szervezetei és a nemzetközi légi közlekedési szervezetek milyen mélységgel foglalkoznak a szektor kiberbiztonságával, és milyen szintű választ adnak ezek a dokumentumok az előzőleg azonosított biztonsági fenyegetésekre.

Repülőtér-generációk

A repülőterek osztályozása egy folyamatosan fejlődő terület, amely az utóbbi években kiemelt figyelmet kapott a légi közlekedési iparágban. Az osztályozási rendszer nem csupán a repülőterek fizikai infrastruktúráját és elhelyezkedését veszi alapul, hanem egyre inkább a technológiai fejlettséget, az utasokkal való interakció minőségét és az üzemeltetési hatékonyságot is figyelembe veszi. Ahogy a világ digitalizálódik, úgy válnak a repülőterek is egyre „okosabbá", integrálva a legújabb technológiai

innovációkat nemcsak az operatív hatékonyság, de az utasélmény javítása érdekében is. Ebben a kontextusban a repülőterek osztályozása átfogó keretrendszert nyújt, amely bemutatja, hogyan fejlődhetnek és alkalmazkodhatnak a repülőterek az új kihívásokhoz és technológiákhoz. Az osztályozás négy fő kategóriába sorolja a repülőtereket az 1.0-tól a 4.0-ig, ahol az 1.0 a legkevésbé fejlett, míg a 4.0 a legmodernebb, okosrepülőtereket jelöli.

Az 1.0-s besorolású repülőterek az alapvető szolgáltatások biztosítására összpontosítanak, mint amilyen a biztonságos és hatékony repülőgép-működtetés, áruszállítás, utasfelvétel, biztonság, poggyászkezelés, miközben igyekeznek minimalizálni a késéseket és az operatív zavarokat. „A repülőterek fejlettebb műveleteket végeznek, de nem fordítanak kellő figyelmet az utasok igényeire" – állítják Alansari és munkatársai kutatásukban.[2] A repülőtéri érdekeltek csak minimális adatot osztanak meg, és a lehető legalacsonyabb szintű együttműködést valósítják meg.

A 2.0-s besorolású repülőterek a modern technológiák alkalmazásával képesek az operatív változásokra reagálni, az adatok megfelelő mennyiségének jelenléte és az érdekelt felek közötti gyors információcsere révén. A repülőterekben megjelennek automatizmusok, de az egyes rendszerek főleg szigetszerűen, egymástól elszigetelten működnek. Ezeken a repülőtereken az egyes bérlők például olyan technológiákat vehetnek igénybe, mint wifi, széles sávú internet és videómegfigyelési szolgáltatások, anélkül, hogy saját megoldásaikat kellene szervezniük és karbantartaniuk.[3]

A 3.0-s besorolású repülőterek modern technológiákkal és jellemzőkkel rendelkeznek. A Cisco Smart Airports tanulmánya[4] szerint a rendszerek egy „digitális rács" köré épülnek, amely lehetővé teszi a magas sebességű széles sávú adatforgalmat az egész ökoszisztémában, beleértve az egyes szereplők között, például repülőtér-üzemeltető, légitársaságok, légiforgalom-irányítás. Az egyes folyamatok hatékonyságát az információ és adatok valós idejű cseréje javítja, amely során az egyes rendszerek folyamatos és nagyszámú adatkapcsolatokkal operálnak,[5] így lehetővé válik jobb és gyorsabb döntések meghozatala. A 3.0-s besorolású repülőterek az utasélményre koncentrálnak, ahol az utasok profitálnak az utasadatok cseréjéből, lehetővé téve számukra, hogy személyre szabott szolgáltatásokat kapjanak.

A 4.0-s besorolású repülőtér koncepciója az Open Data és a Linked Data elveken nyugszik. Az adatoknak integrálódniuk kell egymással, hogy kompatibilis struktúrával rendelkezzenek. A biztonság az egyik legfontosabb szempont. Az adatokat a hatályos jogszabályoknak megfelelően kell védeni. Az érzékeny adatokhoz csak a rendszer jogosult felhasználói férhetnek hozzá. Az Open Data elv alapgondolata az adatok bővítésének és megosztásának lehetősége a jogosult felhasználók között, így mindenki számára elérhetővé téve azokat.[6]

A SITA felmérése[7] alapján is látható, hogy a repülőterek folyamatos beruházásokat hajtanak végre az IT-megoldásaik terén. Az elemzésből jól kiolvasható, hogy a repülőterek

[2] Alansari–Soomro–Belgaum 2019.
[3] Fattah et al. 2009.
[4] Fattah et al. 2009.
[5] Blondel–Zintel–Suzuki 2015.
[6] Nau–Benoit 2017.
[7] SITA 2023.

technológiai fejlődése dinamikus és folyamatos, ahol az IT-kiadások jelentős növekedése az innováció iránti elkötelezettség fokát mutatja. Az utóbbi években megfigyelhető, hogy az üzemeltetési *(opex)* és a tőkeberuházási *(capex)* költségek egyensúlyba kerültek, ami a repülőtéri iparág fejlődési és beruházási hajlandóságát jelzi, nem csupán a meglévő infrastruktúra fenntartását célozzák meg a repülőterek. Különösen 2022-ben az IT-költségek túlszárnyalták az előrejelzéseket, elérve a repülőtéri bevételek 7,17%-át, ami jelzi a tőkeberuházások intenzív növekedését. Ez a tendencia folytatódhat, 2023-ra az elemzésbevételek még nagyobb, 7,45%-os részét kitevő IT-kiadásokra számítottak. A repülőterek stratégiailag fontosnak tartják az adattárházakba, üzletiintelligencia-szoftverekbe, biometrikus azonosító rendszerekbe, valamint az 5G kommunikációs technológiákba történő befektetést. A határellenőrzési folyamatban a legelterjedtebb a biometrikus azonosítás, de a közeljövőben a repülőterek tervezik ezen technológiát más repülőtéri folyamatokba is integrálni. Ezzel párhuzamosan a mesterséges intelligencia és üzleti intelligencia területén a repülőterek stratégiailag fontosnak tartják a startupvállalkozásokkal való együttműködést.

Okosrepülőterek főbb rendszerei és azok kihívásai

Rendszerelem-áttekintés

Az okosrepülőterek rendszereinek azonosítása során azokat elemezzük, amelyek a légi közlekedéssel kapcsolatos specifikus célokat és funkciókat szolgálnak ki. Jelen vizsgálat hatóköréből kikerülnek azok az általános rendszerek, amelyek nem szektorspecifikus feladatokat látnak el, mint például vállalatirányítási rendszerek, épületüzemeltetési rendszer, általános IT-infrastruktúra-rendszerek, mivel a cikk célja az, hogy mélyreható és releváns ismereteket nyújtson egy szűkebb, de kritikus területről. Az általános használatú rendszerek kizárása lehetővé teszi a szerzőnek, hogy fókuszáltabb elemzést végezzen az okosrepülőterek információs rendszereiről.

A repülőterek esetében két fő területet tudunk megkülönböztetni, a légi tevékenységekkel összefüggő részleget *(airside)* és a földi tevékenységeket magában foglaló részleget *(landside)*.

Airside

- Légiforgalom-irányítási rendszer. A légiforgalom-irányítási rendszer kulcsfontosságú eleme a repülőtér rendszereinek, mivel alapvető szerepet játszik a légi közlekedés biztonságának, hatékonyságának és zavartalanságának biztosításában. E rendszer felelős a repülőgépek földi mozgásainak és légi útvonalainak koordinálásáért, a légtér és a repülőtéri létesítmények optimális kihasználásáért, valamint a forgalom folyamatos és biztonságos áramlásának fenntartásáért. Ezen a területen is léteznek magasabb szinten automatizált rendszerelemek. Ilyen rendszerelem lehet a pályaelőrejelzés-technológia, ami lehetővé teszi a repülőgépek útvonalának térbeli és időbeli előrejelzését, növelve a repülési

tervek pontosságát és a biztonságot. Ilyen technológia a középtávú konfliktusfelismerés is, ami 0–60 perces időhorizonton belül azonosítja a lehetséges légtérkonfliktusokat.[8]

- Repülőgépek földi kiszolgálása. A földi kiszolgálási feladatokat általában a légitársaság és a szolgáltató közötti szolgáltatási szintű megállapodások határozzák meg, amelyek rögzítik a kívánt terjedelmet, árat, minőségi szintet és kulcsfontosságú teljesítménymutatókat. A földi kiszolgálási tevékenységek két fő kategóriába sorolhatók, úgymint a „szárnyon felüli" és „szárny alatti" tevékenységek. A „szárnyon felüli" tevékenységek a repülőgép utasterével kapcsolatosak, és magukban foglalják az utasok beszállását és leszállását, az étkeztetést, a kabin tisztítását és előkészítését, valamint szükség szerint a biztonsági és védelmi ellenőrzéseket. A „szárny alatti" tevékenységek a rakomány (konténeres és ömlesztett) kirakodására és berakodására, valamint egyéb földi tevékenységekre összpontosítanak, mint például az áramellátás (*ground power unit,* GPU), a kabinhőmérséklet beállítása, a futóművek rögzítése, az üzemanyag-utántöltés, az ivóvíz- és WC-kiszolgálás, a vontatás és visszatolatás, valamint az utasok feljutásának biztosítása lépcsőkön, rámpákon vagy utasfelszállási hídon keresztül. Azonban ezek automatizálása nem egyszerű, mivel az egyes repülőgépek fizikai adottságai, az automatizált és manuális folyamatok összehangolása mind nagy kihívást tud jelenteni ezen a területen.[9]
- Repülőtéri járművek nyomon követése. Ez a rendszer lehetővé teszi a repülőtéri üzemeltetők számára, hogy valós időben lássák a járművek jelenlegi és korábbi helyzetét, és nyomon kövessék az erőforrások felhasználását. A rádiófrekvenciás azonosítás (*radio frequency identification,* RFID) címkékkel ellátott vészhelyzeti járműveket is figyeli, ami hozzájárul a gyorsabb válaszidőkhöz, mivel az incidensparancsnokok és a mentőegységek azonnal információt kapnak a leggyorsabb útvonalakról.[10]

Landside

- Okosbecsekkolás. Az utasok a check-in során többféle módszert is használhatnak, többek között weboldalas megoldást, mobiltelefonos applikációt és számítógépes kioszkokat. Ezekkel a megoldásokkal csökkenteni lehet a földi kiszolgáló személyzet emberi közreműködését, és ezáltal a légitársaságok képesek csökkenteni a költségeiket, illetve a személyzet által elkövetett hibákat. Az okosrepülőterek összekapcsolták a működő légitársaságok összes kioszkját, és az utasok a terminálon elhelyezett bármelyik közös kioszkon keresztül bejelentkezhetnek.[11]
- Önálló beszállás. A beszállási folyamat számos manuális részből áll, amelyben személyzeti interakció szükséges. A beszállást segítő és ellenőrző rendszerek

[8] Bestugin et al. 2020.
[9] Tabares – Mora-Camino 2019.
[10] Marks–Rietsema 2014.
[11] Wittmer 2011.

segítik ezen folyamat automatizálását úgy, hogy a kapuknál elhelyezett beszállókártya-olvasók lehetővé teszik, hogy az utasok saját maguk olvassák be a beszállókártyájukat. Így emberi ellenőrzés nélkül, az RFID-olvasási technológiát használva szállhatnak fel a repülőgépre. A beszállókártya beolvasása után a kapuk automatikusan kinyílnak, és az utasok beléphetnek a repülőgépbe. Emberi beavatkozás csak a földi személyzet által végzett felügyelet során szükséges.[12]

- Beltéri navigálás és további utaskezelés. A mobilapplikációk segíthetnek az utasoknak a repülőtéren belüli navigálásban,[13] illetve csatorna lehet az utas és a terminál személyzete között az egyes fontos információk átadására, mint például járatkésés.[14]
- Határellenőrzés. A kézipoggyász ellenőrzésére szolgáló robbanóanyag-felderítő rendszerek (*explosive detection systems for cabin baggage screening,* EDCSB) röntgensugaras technológiát és mesterséges intelligenciát használnak a robbanóanyagok azonosítására és elkülönítésére a poggyász röntgenfelvételein. Az EDCSB-rendszerek automatikusan meg tudják határozni, hogy a poggyász tartalmaz-e veszélyes anyagokat.[15]
- Az e-kapuk használata során az utasok személyzeti beavatkozás nélkül képesek személyazonosságukat validálni. Az útlevél-azonosító megadását, illetve a biometrikus azonosítást követően lehet áthaladni.[16]
- Poggyászkezelés. A rádiófrekvenciás azonosítás (RFID) és a vezeték nélküli érzékelőhálózatok integrációja lehetővé teszi egy olyan rakományfelügyeleti rendszer létrehozását, amely a zökkenőmentes működés elősegítése érdekében valós idejű nyomon követést és a repülőtéri rakomány helymeghatározását képes megvalósítani. Az RFID a poggyászok címkézésére is használható, az összegyűjtött információkat pedig egy IoT-felhőszerverben tárolják, hogy az adatok a különböző repülőtereken könnyen visszakereshetők legyenek. Mobilalkalmazásokkal integrálva az utasok mobilkészülékeik segítségével pontosan nyomon követhetik csomagjaik helyét, és csökkenthetik az elveszett poggyászok számát.[17]
- AODBS *(Airport Operations Database System)*. A repülőtéri adatbázis operációs rendszer egy speciális szoftverplatform, amelyet a repülőterek használnak különféle adatok kezelésére, tárolására és feldolgozására. Ezek az operációs rendszerek központi szerepet játszanak a repülőtér működésében, mivel lehetővé teszik az adatok hatékony és biztonságos kezelését, és támogatják a különféle repülőtéri szolgáltatások integrációját. Egy ilyen rendszerben a következő adatok jelenhetnek meg:

[12] Rajapaksha–Jayasuriya 2020.
[13] Mantouka et al. 2018.
[14] AlMashari et al. 2018.
[15] Hättenschwiler et al. 2018.
[16] del Río et al. 2016.
[17] Wang 2018.

a) Repülési információk kezelése: az AODBS tárolja a járatokkal kapcsolatos összes fontos információt, beleértve a járatmenetrendeket és a járatok kapuhoz rendelését. Ez a rendszer biztosítja, hogy a járatok időben és hatékonyan legyenek kezelve.
b) Erőforrás-kijelölés: az AODBS felelős a repülőtéri erőforrások, mint például a kapuk, check-in pultok és beszállókapuk kijelöléséért és kezeléséért. Ez segít optimalizálni a repülőtér működését, és biztosítja az erőforrások hatékony felhasználását.
c) Diagramok és statisztikai jelentések készítése: az AODBS lehetővé teszi különböző diagramok és statisztikai jelentések készítését, amelyek segítenek a repülőtér üzemeltetésének elemzésében és optimalizálásában.[18]

Látható, hogy az okosrepülőterek főbb ismérve a különböző rendszerek közötti magas szintű interoperabilitás. A magas szintű kapcsolódás alapja a rendszerek rendszere (*system of systems,* SoS) koncepciójának a megléte. Az SoS a rendszerek összességét egyesíti egy olyan feladathoz, amelyet egyik rendszer sem képes egyedül elvégezni. Az egyes rendszerelemek megtartják saját kezelésüket, céljaikat és erőforrásaikat, miközben az SoS-on belül együttműködnek, és alkalmazkodnak az SoS céljainak eléréséhez.[19]

Okosrepülőterek kiberbiztonsági kihívásai

Az ENISA tanulmánya,[20] illetve a Georgia Lykou és társai[21] által publikált tanulmány azonosította azokat a fenyegetési kategóriákat, amelyek hatással lehetnek az okosrepülőterekre:

- Hálózati és kommunikációs támadások. A hálózatok rosszindulatú forrásokból érkező támadásoknak vannak kitéve, amelyek passzív és aktív kategóriákba sorolhatók. A passzív támadások esetén az adatokat lehallgatják, míg az aktív támadások során a hálózat normál működését zavarják meg, és hozzáférést szereznek a hálózati eszközökhöz. Annak ellenére, hogy az egyes protokollok megpróbálják megakadályozni a kommunikáció lehallgatását, az intelligens repülőterek még mindig vonzó célpontok a manipulációs vagy hálózati támadásokhoz. A vezeték nélküli kommunikáció, a légi forgalmi irányítás rádiójelei is veszélyeztetettek lehetnek, amelyeket zavaró eszközökkel befolyásolnak. A szolgáltatásmegtagadási támadások (*denail of service,* DoS) további kockázatot jelentenek, mivel megzavarhatják az információs rendszereket és a hálózatokat, ami komoly hatással lehet a repülőtéri rendszerekre és az utasokra.
- Rosszindulatú szoftverek. A rosszindulatú szoftverek, amelyek megfertőzhetik az általános információs rendszereket, veszélyeztethetik az intelligens eszközöket, beleértve az utasok és a személyzet mobil eszközeit, valamint a repülőtéri

[18] Yang 2010.
[19] Sharkov 2017.
[20] ENISA 2018.
[21] Lykou–Anagnostopoulou–Gritzalis 2018.

infrastruktúra rendszereit. Az ilyen szoftverek rosszindulatú viselkedést mutatnak, visszaélve a környezeti jogosultságokkal, és súlyos hatással lehetnek a repülőtéri rendszerekre. Az intelligens repülőtéri rendszerekben fennálló sebezhetőségek miatt a rosszindulatú szoftveres támadások potenciális veszélyt jelentenek.

- A repülőtéri eszközök manipulációja. A repülőtéri eszközök manipulálásának különféle módjai veszélyeztethetik a repülőtéri infrastruktúrát. A központi foglalási rendszerek, az adminisztrációs informatikai rendszerek és a tárolt érzékelőadatok manipulálása súlyos következményekkel járhat, beleértve a fizikai biztonság megsértését is.
- A jogosultsággal való visszaélés. A hozzáférés-ellenőrzések ellenére a támadók képesek lehetnek hitelesítő adatokat megszerezni és jogosultsági jogokat kiterjeszteni. Még a bennfentes fenyegetésként fellépő alkalmazottak vagy vállalkozók is visszaélhetnek jogosultságaikkal, például hitelesítő adatok lopásával vagy social engineering technikákkal.
- Social engineering és adathalász-támadások. A social engineering módszereivel az embereket lehet manipulálni vagy félrevezetni, ami átjutást biztosít a rendszerbe. Az e-mail továbbra is az elsődleges módszer a támadók számára, lehetővé téve számukra az áldozatok fiókjainak, személyazonosságának és jogosultságának megszerzését.

A Georgia Lykou és társai[22] által publikált cikkben egy kérdőíves felmérést ismertettek, amelyben 34 európai, illetve amerikai repülőteret elemeztek. A cikk egy felmérést is tartalmazott, hogy az okosrepülőterek esetében az IoT-eszközök alkalmazása a SCADA-rendszereken keresztül, az air- és landside területeken át mindenhol megtalálható. A cikkből az is látható, hogy az okosrepülőtereket érintő fenyegetések az airside és landside rendszerek esetében is megjelennek, tehát a legtöbb repülőtéri rendszerre hatással vannak. Ez azért lehetséges, mert az okosrepülőterek esetében a rendszerintegráció igen nagy számban jelenik meg a legkülönbözőbb szinteken az IoT-eszközök segítségével, így létrehozva az SoS-architektúrát. Az SoS-ökoszisztéma elemeiben egyetlen sebezhetőség kihasználásával akár az egész összekapcsolt architektúrát veszélyeztetni lehet, így akár egy poggyászkezelő rendszerben megjelenő IoT-eszköz sérülékenysége kihatással lehet a repülőgép berakodására is.[23]

A légi közlekedés kiberbiztonságát érintő nemzetközi dokumentációk áttekintése

Jelen fejezetben megvizsgálom azokat a dokumentumokat, amelyeket az Egyesült Államok és az Európai Unió szervezetei bocsátottak ki. Ezenfelül azokat a dokumentumokat is, amelyeket valamely nemzetközi szervezet publikált a polgári légi közlekedés kiberbiztonságával kapcsolatban.

[22] Lykou–Anagnostopoulou–Gritzalis 2018.
[23] Sharkov 2017.

Azért az Egyesült Államokat, illetve az Európai Uniót választottam mint elemzésem célpontjai, mivel e két terület tagállamai rendelkeznek a legnagyobb utasforgalmat kiszolgáló repülőterekkel. A Nemzetközi Polgári Repülési Szervezet 2022-es légi közlekedési statisztikai eredményeiből az látható, hogy a világ utasfogalom alapján 25 legnagyobb repülőteréből 19 reptér vagy az USA-ban, vagy az Európai Unióban található.[24]

Az egyes dokumentumokat az alapján értékeltem, hogy milyen szinten jelennek meg bennük kiberbiztonsági követelmények/ajánlások. Az alábbi értékelési módszert alkalmaztam:

- Érintőleges: olyan dokumentum, amely megemlíti a kiberbiztonság fontosságát, azonban azon belül nem jelöl meg specifikus területet.
- Alapszintű: olyan dokumentum, amely a kiberbiztonsági szabályozás valamelyik aspektusát kifejti, azonban csak irányelveket, illetve magas szintű szabályozásokat/ajánlásokat tartalmaz.
- Átfogó: a kiberbiztonság legtöbb területével kapcsolatosan határoz meg magas szintű szabályozásokat/ajánlásokat.
- Részletes: olyan dokumentum, amely a kiberbiztonság legtöbb területével kapcsolatosan részletes szabályozást/ajánlásokat tartalmaz. Ezen felül azon dokumentumok, amelyek a kiberbiztonság valamelyik területével kapcsolatban fogalmaznak meg részletes követelményeket/ajánlásokat. Alapul véve ezeket, részletes szabályokat lehet kialakítani az információbiztonság területén.

Az 1. táblázatban jogszabályi szinten csak hatályban lévő dokumentumok jelennek meg, mivel csak azoknak a tartalma kötelező érvényű.

1. táblázat: A légi közlekedés kiberbiztonságával kapcsolatos nemzetközi dokumentumok vizsgálatai

Szabályozás /Szabvány/ Ajánlás neve	**Leírás**	**Követelmények absztrakciós szintje**	**Dokumentum típusa**	**Hatókör/ Kiadó**
Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete[25]	Polgári légi közlekedés területén alkalmazandó közös szabályok meghatározása.	Érintőleges	jogszabály	Európai Unió/ Európai Parlament és a Tanács

[24] ICAO 2022a.

[25] Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete (2018. július 4.) a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
Az Európai Parlament és a Tanács 376/2014/EU rendelete[26]	A polgári légi közlekedésben előforduló események jelentéséről, elemzéséről és nyomon követéséről.	Érintőleges	jogszabály	Európai Unió/ Európai Parlament és a Tanács
A Bizottság (EU) 2022/1645 felhatalmazáson alapuló rendelete[27]	Az (EU) 2018/1139 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról a potenciális hatással járó információbiztonsági kockázatok kezelésére vonatkozó követelmények.	Átfogó szintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács
Az Európai Parlament és a Tanács (EU) 2022/ 2555 irányelve (NIS 2)[28]	A NIS 2 irányelv két kulcsfontosságú területre összpontosít: a kiberbiztonsági felügyeletre és a kiberbiztonsági tanúsításra. Ezek a területek az Európai Unióban a kiberbiztonság magas szintjének biztosítását és a digitális szolgáltatások iránti bizalom növelését szolgálják. Kiberbiztonsági Felügyelet: Az irányelv előírja a kiberbiztonsági felügyeletért felelős nemzeti hatóságok létrehozását. Ezek a hatóságok felügyelik a kiberbiztonsági követelményeknek való megfelelést. Az alapvető és fontos szervezetek kategóriákba sorolása alapján történik a felügyelet. Az alapvető fontosságú szervezetek, ilyenek például a repülőterek, szigorúbb felügyelet alá esnek. Kiberbiztonsági szabályozás terén átfogó, magas szintű követelményeket fogalmaz meg a hatálya alá eső szervezetekkel szemben. Jelen jogszabály terméktanúsítási része nem érvényes a légi közlekedési ágazatra.	Átfogó szintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács

[26] Az Európai Parlament és a Tanács 376/2014/EU rendelete (2014. április 3.) a polgári légi közlekedési események jelentéséről, elemzéséről és nyomon követéséről, valamint a 996/2010/EU európai parlamenti és tanácsi rendelet módosításáról és a 2003/42/EK európai parlamenti és tanácsi irányelv, valamint az 1321/2007/EK bizottsági rendelet és az 1330/2007/EK bizottsági rendelet hatályon kívül helyezéséről EGT-vonatkozású szöveg.

[27] A Bizottság (EU) 2022/1645 felhatalmazáson alapuló rendelete (2022. július 14.) az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek a 748/2012/EU és a 139/2014/EU bizottsági rendelet hatálya alá tartozó szervezetekre vonatkozó, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésével kapcsolatos követelmények tekintetében történő alkalmazására irányadó szabályok megállapításáról, valamint a 748/2012/EU és a 139/2014/EU bizottsági rendelet módosításáról.

[28] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv).

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
Az Európai Parlament és Tanács (EU) 2018/1139 rendelete[29]	A légiközlekedési tanúsítás a NIS 2 hatálya alól kivételt képez, mert ezen területet jelen rendelettel tervezik lefedni a jogalkotók. Az IKT-rendszerek tanúsítása magában foglalja annak biztosítását, hogy ezek a rendszerek megfeleljenek a szigorú biztonsági és védelmi előírásoknak a balesetek, incidensek és a légi forgalmi műveletek zavarainak megelőzése érdekében. A rendelet hangsúlyozza az IKT-rendszerek, termékek és komponensek alapos értékelésének fontosságát a biztonsági követelményeknek való megfelelés ellenőrzése és a repülési tevékenységekben való alkalmazásukkal kapcsolatos potenciális kockázatok mérséklése érdekében. Viszont a kiberbiztonság csak magas szinten jelenik meg a dokumentumban.	Alapszintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács
A Bizottság (EU) 2015/1998 végrehajtási rendelete[30]	A légiközlekedés-védelmi közös alapkövetelmények végrehajtására vonatkozó részletes intézkedések megállapításáról szóló jogszabály, amely közvetlenül nem azonosít specifikus kiberbiztonsági követelményt. Azonban számos olyan kontrollt határoz meg, amelyet egy IKT-eszköz biztosít, illetve fizikai biztonsági követelmény is szerepel ezen jogszabályban.	Alapszintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács
A Bizottság (EU) 2019/1583 végrehajtási rendelete[31]	A 2015/1998 végrehajtási rendeletet bővíti ki külön kiberbiztonsági követelményekkel.	Alapszintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács

[29] Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete (2018. július 4.) a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről.

[30] A Bizottság (EU) 2015/1998 végrehajtási rendelete (2015. november 5.) a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról.

[31] A Bizottság (EU) 2019/1583 végrehajtási rendelete (2019. szeptember 25.) a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról szóló (EU) 2015/1998 végrehajtási rendeletnek a kiberbiztonsági intézkedések tekintetében történő módosításáról.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
A Bizottság (EU) 2017/373 végrehajtási rendelete[32]	A rendeletben magas szinten jelenik meg kiberbiztonság. A dokumentumban a védelemirányítási rendszer előírja, hogy a légi navigációs szolgáltatók, a légi forgalmi áramlásszervezés szolgáltatói és a hálózatirányítók megtegyék a szükséges intézkedéseket rendszereik, rendszerelemeik és adataik védelme érdekében az olyan információ- és kiberbiztonsági kockázatokkal szemben, amelyek jogosulatlan beavatkozást jelenthetnek a szolgáltatás nyújtásában.	Érintőleges	jogszabály	Európai Unió/ Európai Parlament és a Tanács
A Bizottság (EU) 2023/203 végrehajtási rendelete[33]	Potenciális hatással járó információbiztonsági kockázatok kezelésére vonatkozó követelmények tekintetében.	Alapszintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács
A Bizottság (EU) 2023/1769 végrehajtási rendelete[34]	A légi forgalmi irányítási/légi navigációs szolgálati rendszerek és rendszerelemek tervezésében vagy gyártásában részt vevő szervezetek jóváhagyására vonatkozó műszaki követelmények és igazgatási eljárások megállapításáról.	Alapszintű	jogszabály	Európai Unió/ Európai Parlament és a Tanács

[32] A Bizottság (EU) 2017/373 végrehajtási rendelete (2017. március 1.) a légiforgalmi szolgáltatást/léginavigációs szolgálatokat és más légiforgalmi szolgáltatási hálózati funkciókat és azok felügyeletét ellátó szolgáltatókra vonatkozó közös követelmények meghatározásáról, valamint a 482/2008/EK rendelet, az 1034/2011/EU, az 1035/2011/EU és az (EU) 2016/1377 végrehajtási rendelet hatályon kívül helyezéséről, továbbá a 677/2011/EU rendelet módosításáról.

[33] A Bizottság (EU) 2023/203 végrehajtási rendelete (2022. október 27.) az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU és az (EU) 2015/340 bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet hatálya alá tartozó szervezetek, valamint a 748/2012/EU, az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU, az (EU) 2015/340 és a 139/2014/EU bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet hatálya alá tartozó illetékes hatóságok tekintetében a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésére vonatkozó követelmények tekintetében történő alkalmazására vonatkozó szabályok megállapításáról, valamint az 1178/2011/EU, a 748/2012/EU, a 965/2012/EU, a 139/2014/EU, az 1321/2014/EU és az (EU) 2015/340 bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet módosításáról.

[34] A Bizottság (EU) 2023/1769 végrehajtási rendelete (2023. szeptember 12.) a légiforgalmi szolgáltatási/léginavigációs szolgálati rendszerek és rendszerelemek tervezésében vagy gyártásában részt vevő szervezetek jóváhagyására vonatkozó műszaki követelmények és igazgatási eljárások meghatározásáról, valamint az (EU) 2023/203 végrehajtási rendelet módosításáról.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
Elsődleges, könnyen hozzáférhető szabályok az információbiztonságért[35]	Ez a dokumentum részletes követelménykatalógust tartalmaz a légi közlekedés szereplőinek. Ennek alapja ezen ágazat esetében megjelenő jogi szabályozás. Azonban a jogszabályok csak főbb követelményeket határoznak meg. Ezzel a dokumentummal biztosítani lehet a magasan megfogalmazott elvárásoknak való megfelelést.	Részletes	ajánlás	Európai Unió/ Európai Unió Repülésbiztonsági Ügynökség
A légi forgalmi irányítás kiberbiztonsági érettségi modellje[36]	A dokumentum az Eurocontrol által meghatározott érettségi rendszert írja le. Ez alapján pontosan azonosítható, hogy az adott szervezet az információbiztonság egyes területét milyen érettségi szinten üzemelteti.	Részletes	felmérő módszertan	Európai Unió/ Eurocontrol
Okosrepülőterek biztonsága[37]	Az ENISA dokumentuma átfogó elemzést nyújt az okosrepülőterek felépítéséről és azon fenyegetésekről, amelyeket számításba kell vennie ezen létesítményeknek. Azonosít különböző szcenáriókat, amelyek az egyes fenyegetések bekövetkezéséhez köthetők. Illetve tartalmaz egy követelménykatalógust is, amely azonosítja a kiberbiztonság egyes területeinek főbb követelményeit.	Részletes	publikáció	Európai Unió/ Európai Unió Kiberbiztonsági Ügynöksége
Repülési kiberbiztonsági stratégia[38]	A Nemzetközi Polgári Repülési Szervezet (ICAO), az Egyesült Nemzetek Szervezetének ügynöksége kiadott 2019-ben egy kiberbiztonsági stratégiát. A stratégia a következő hét pillérre épülő keretrendszer: nemzetközi együttműködés; irányítás; hatékony jogszabályok és szabályozások; kiberbiztonsági politika; információmegosztás; incidenskezelés és vészhelyzeti tervezés; és kapacitásépítés, képzés és kiberbiztonsági kultúra.	Alapszintű	stratégia	Nemzetközi/ Nemzetközi Polgári Repülési Szervezet

[35] EASA 2023.
[36] Eurocontrol 2019.
[37] ENISA 2018.
[38] ICAO 2019.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
Kiberbiztonsági cselekvési terv, 2. kiadás[39]	A dokumentum az EASA által kiadott útmutató, amely az Európai Unió 2023/203 és 2022/1645 rendeletei alapján készült. Célja az információbiztonsági kockázatok kezelése a légi közlekedési szektorban, tartalmazza az ISMS bevezetésének és fenntartásának követelményeit, incidens kezelésére vonatkozó irányelveket, valamint példákat a fenyegetési forgatókönyvekre. Emellett részletezi az egyes információbiztonsági feladatokat, az azok ellátásához szükséges személyzeti követelményeket és képzettségi elvárásokat, segítve ezzel a biztonság fenntartását és növelését.	Átfogó	cselekvési terv	Nemzetközi/ Nemzetközi Polgári Repülési Szervezet
Kiberbiztonsági kultúra a polgári repülésben[40]	A dokumentum útmutatást nyújt a tagállamok és az érdekelt felek számára a polgári légi közlekedési ágazat szervezetein belül a szilárd kiberbiztonsági kultúra kialakításához. A dokumentum hangsúlyozza a szervezeti kultúra jelentőségét a kiberbiztonságban, valamint a személyzet folyamatos képzését és támogatását a kiberbiztonsági kockázatok kezelésében és az ágazat ellenálló képességének fokozásában.	Részletes	útmutató	Nemzetközi/ Nemzetközi Polgári Repülési Szervezet
Kiberbiztonsági stratégiai iránymutatás[41]	A dokumentum célja egy átfogó globális kiberbiztonsági stratégia megalkotása a polgári repülés területén. Az ICAO (International Civil Aviation Organization – Nemzetközi Polgári Repülési Szervezet) felismeri a kibertámadások növekvő fenyegetését, amelyek különböző területeken egyszerre hathatnak és gyorsan terjedhetnek. Az új stratégia célja, hogy a polgári repülési szektor ellenálló legyen a kibertámadásokkal szemben, és világszerte biztonságos és megbízható maradjon, miközben tovább fejlődik és növekszik. E cél elérése érdekében az ICAO hangsúlyozza az államok közötti együttműködés fontosságát, a megfelelő törvényhozás és szabályozás megteremtését, az információmegosztást, valamint az incidens kezelését és a vészhelyzeti tervezést. A stratégia további kulcselemei közé tartozik a képességfejlesztés, a képzés és a kiberbiztonsági kultúra erősítése.	Átfogó	útmutató	Nemzetközi/ Nemzetközi Polgári Repülési Szervezet

[39] ICAO 2022b.
[40] ICAO 2022c.
[41] ICAO 2022d.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
Útmutató a jelzőlámpás eljáráshoz[42]	A Nemzetközi Polgári Repülési Szervezet ezen dokumentumban egy olyan jelzőrendszer alkalmazását írja le, amely segítségével a kibertérben kezelt, továbbított adatokra a szenzitivitásuk és értékük alapján kell szabályokat kialakítani.	Átfogó	útmutató	Nemzetközi/ Nemzetközi Polgári Repülési Szervezet
Elnöki szakpolitikai irányelv – létfontosságú infrastruktúrák biztonsága és ellenálló képessége[43]	Azonosítja a közlekedési ágazatot mint kritikus infrastruktúrát, és magas szintű irányelveket tartalmaz. Tehát a légi közlekedés csak közvetetten jelenik meg benne.	Érintőleges	irányelv	Egyesült Államok/ Fehér Ház
H.R.302 – Az FAA 2018. évi újbóli felhatalmazásáról szóló törvény[44]	Intézkedéseket tartalmaz a repülési szektor kiberbiztonságának a fejlesztésére az alábbi pontokban: légi forgalmi irányítási rendszerben azonosított kiberbiztonsági sebezhetőségek megszüntetése; a kiberbiztonságnak az okosrepülőtér kezdeményezés alapelemének kell lennie; pilóta nélküli légi járművek kiberbiztonsága; a Szövetségi Légügyi Hivatal integrált tesztkörnyezetet alakítson ki a légi forgalmi irányítás modernizációs technológiáinak kutatására, fejlesztésére, értékelésére és validálására.	Alapszintű	jogszabály	Egyesült Államok/ Kongresszus
AC 119-1A – A légijármű-hálózat biztonsági program működési engedélyezése[45]	Tanácsadó körlevél, részletesen leírja, hogyan lehet megszerezni a repülőgépek üzemeltetési engedélyét, amelyek a fedélzeti számítógépes hálózat biztonságával kapcsolatos különleges feltétel alapján kaptak tanúsítványt. Ezen dokumentumban az információbiztonságok elleni védelem, illetve az eseménykezelés is megjelenik mint szempont.	Alapszintű	tanácsadói körlevél	Egyesült Államok/ Szövetségi Légi Közlekedési Hatóság

[42] ICAO 2022e.
[43] Presidential Policy Directive/PPD-21 – Critical Infrastructure Security and Resilience.
[44] H.R.302 – An act to provide protections for certain sports medicine professionals, to reauthorize Federal aviation programs, to improve aircraft safety certification processes, and for other purposes.
[45] AC 119-1A – Operational Authorization of Aircraft Network Security Program.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
A Közlekedésbiztonsági felügyelet kiberbiztonsági ütemterve[46]	A Közlekedésbiztonsági felügyelet kiberbiztonsági ütemterve a Belbiztonsági Minisztérium kiberbiztonsági stratégiájához közvetlenül igazodó keretrendszert biztosít, amely alapján a Közlekedésbiztonsági felügyeletnek a következő öt évben végre kell hajtania kiberbiztonsági feladatait. A felügyelet évente felülvizsgálja és frissíti az ütemterv végrehajtási tervét. A dokumentum a következő pilléreken alapszik: kockázatazonosítás, sebezhetőség csökkentése, fenyegetés csökkentése, következmények enyhítése.	Átfogó	ütemterv	Egyesült Államok/ Közlekedésbiztonsági felügyelet
Szövetségi légi közlekedési hatóság Kiberbiztonsági stratégiája[47]	A dokumentum a (Federal Aviation Administration – FAA) 2018-as Reauthorization Act 509. szakasza alapján készült jelentés, amely áttekinti és frissíti az FAA kiberbiztonsági stratégiáját. A jelentés kiemeli a stratégia öt alappillérét, amelyek célja az FAA hálózatainak és rendszereinek védelme, az adatvezérelt kockázatkezelési képességek fejlesztése, a munkaerő kiberbiztonsági képességeinek építése, valamint a kormányzati és ipari partnerekkel való együttműködés fenntartása és fejlesztése. A dokumentum bemutatja a 2019-es felülvizsgálat eredményeit, az azóta történt fejlesztéseket, és az új technológiák, például a felhőszolgáltatások integrálását a stratégiába.	Alapszintű	stratégia	Egyesült Államok/ Szövetségi Légügyi Hivatal
Közlekedési rendszerek ágazatspecifikus terv[48]	Megjelenik a légi közlekedési ágazat mint kritikus infrastruktúra, és azonosítja azok résztvevőit, többek között a repülőtereket is. Azonosítja a biztonsági kihívásokat, megjelenik a kiberbiztonsági fenyegetés mint fogalom. Azonosítja a célokat és prioritásokat is a biztonsággal kapcsolatban.	Alapszintű	terv	Egyesült Államok/ Amerikai Kibervédelmi Ügynökség

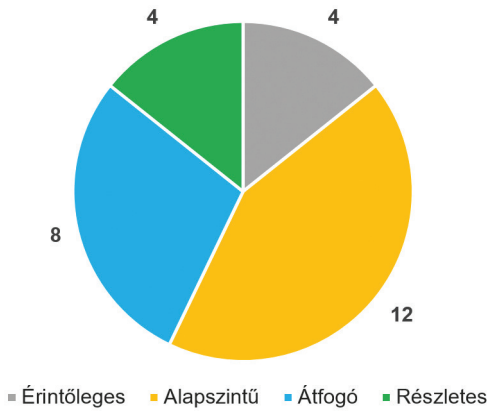
[46] TSA 2018.
[47] FAA 2020.
[48] CISA 2015.

Szabályozás /Szabvány/ Ajánlás neve	Leírás	Követelmények absztrakciós szintje	Dokumentum típusa	Hatókör/ Kiadó
CANSO kiválósági szabvány a kiberbiztonság terén[49]	A Polgári Légiforgalmi Szolgálatok Szervezete (Civil Air Navigation Services Organization, CANSO) Biztonsági Állandó Bizottságának kiberbiztonsági munkacsoportja (Cyber Safety Task Force, CSTF) készítette. Célja egy átfogó kiberbiztonsági érettségi keretrendszer biztosítása a navigációs szolgáltatóknak. A keretrendszer az információbiztonság területeit átfogó módon írja le és egyes értettségi szinten értékeli azokat.	Átfogó	szabvány	Nemzetközi/Polgári Légiforgalmi Szolgálatok Szervezete
Légiforgalom-irányítási kiberbiztonsági szabályzat sablon[50]	Alapot biztosít a légi forgalmi irányítóknak, amely alapján egy minden információbiztonsági területre kiterjedő szabályozási rendszert lehet elkészíteni.	Alapszintű	útmutatás	Nemzetközi/Polgári Légiforgalmi Szolgálatok Szervezete
Repülési kiberbiztonsági iránymutatás[51]	Két része van. Az első része kifejezetten a szervezeti kultúrával és hozzállással kapcsolatban fogalmaz meg átfogó követelményeket. Míg a második a repülőgépek kiberbiztonságával és kockázatával fogalmaz meg átfogó szabályozást.	Átfogó	útmutatás	Nemzetközi/Nemzetközi Légi Szállítási Szövetség
Biztonsági irányítási rendszer (SeMS) kézikönyv[52]	Átfogó kockázatmenedzsment, illetve biztonsági keretrendszer kialakítását segíti elő, azonban a kiberbiztonsági területtel érintőlegesen foglalkozik.	Átfogó	szabvány	Nemzetközi/Nemzetközi Légi Szállítási Szövetség

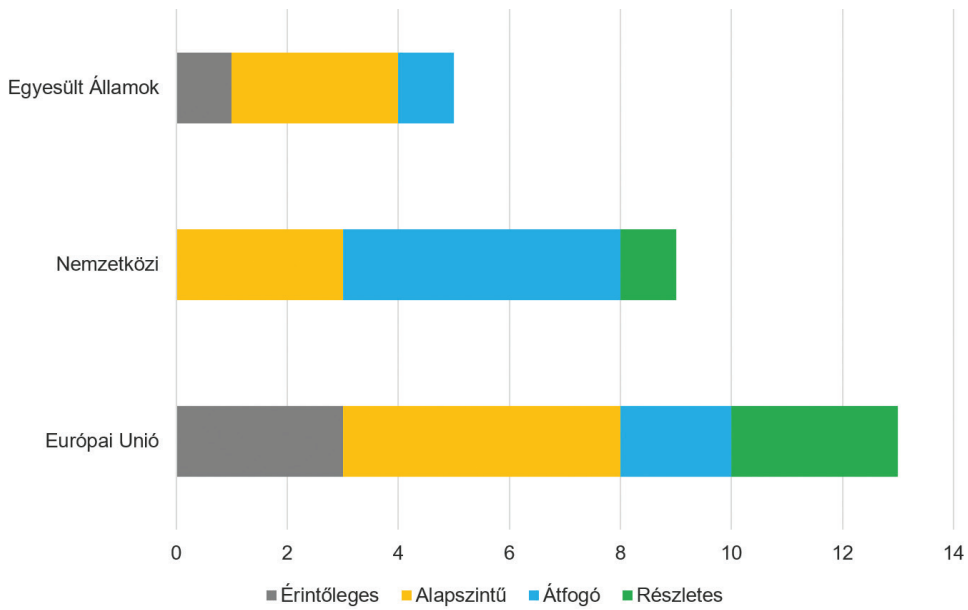
Forrás: a szerző szerkesztése

Összesen 28 dokumentum. Absztrakciós szintjeik vizsgálata során az látható, hogy a legtöbb publikált forrás (12 db) alapszintű szabályokat/ajánlásokat fogalmaz meg a légi közlekedés kiberbiztonságával szemben. Ezt a csoportot követik az átfogó szintű dokumentumok (8 db), majd a részletes (4 db) és az érintőleges (4 db) jelenik meg.

[49] CANSO 2020.
[50] CANSO 2021.
[51] IATA 2021.
[52] IATA 2024.



1. ábra: A dokumentumok absztrakciós szintjeinek megoszlása
Forrás: a szerző szerkesztése



2. ábra: Absztrakciós szint megoszlása területi hatókör szerint
Forrás: a szerző szerkesztése

Ha megvizsgáljuk hatókörszinten az egyes dokumentumokhoz tartozó követelményi absztrakciós szintet, akkor az látható, hogy az Egyesült Államok egyes szervezetei darabszám alapján kevés anyagot bocsátottak ki a témában. Illetve ezen dokumentumok főleg alapszintű követelményeket/ajánlásokat tartalmaznak. Kiemelhető az Európai Unióhoz köthető dokumentumok mennyisége, illetve részletessége. Az EU

számos jogi szabályozásban foglalkozik a légi közlekedés kiberbiztonságával. Szervezetei részletes elemzést, illetve útmutatást nyújtanak a légi közlekedési szereplők, így az okosrepülőterek üzemeltetői számára is. Iránymutatásai nemcsak a legfőbb kockázatokkal foglalkoznak, hanem segítséget nyújtanak egy szervezetszintű információbiztonsági irányítás kialakításához és fenntartásához is. Megállapíthatjuk tehát, hogy az Európai Unió szervezetei több és részletesebb dokumentumot publikáltak a témában. Első hipotézisemet megcáfoltam.

Okosrepülőterek kiberbiztonsági kihívásainak csökkentése a nemzetközi dokumentumok alapján

Vajon az előzőleg megjelölt, okosrepülőterekkel kapcsolatos kiberbiztonsági kihívásokra az azonosított és részletesnek értékelt nemzetközi dokumentumok képesek-e releváns útmutatást adni?

A légi közlekedés kiberbiztonságát érintő nemzetközi dokumentumokat különböző kategóriákba soroltuk. A besoroláskor azt a hatékonyságot vizsgáltuk, hogy a dokumentumok milyen mértékben segítenek az adott fenyegetés kezelésében.

A következő értékelési kategóriákat állítottuk fel:

- Kielégítően segít: a dokumentum teljes mértékben lefedi az adott fenyegetést, beleértve annak felismerését, megelőzését, az azonnali válaszintézkedéseket, valamint a helyreállítási folyamatokat. Minden releváns aspektust részletesen tárgyal, és konkrét, gyakorlati útmutatást nyújt.
  - A következő jellemzőkből többet is tartalmaz az adott dokumentum:
    - Részletes előírások a fenyegetésanalízissel és azonosítással kapcsolatban.
    - Pontosan meghatározza, hogyan lehet hatékony megelőzési és védelmi stratégiát kialakítani.
    - Pontosan meghatározza, hogyan lehet hatékony és azonnali válaszintézkedéseket kialakítani.
    - Pontosan meghatározza, hogyan lehet helyreállítási tervet és folyamatokat kialakítani.
    - Példák és esettanulmányok bemutatása.
- Részben segít: a dokumentum csak részlegesen fedi le az adott fenyegetéseket. Egyes aspektusokat jól kezel, de hiányosságok vannak a fenyegetésazonosítás, a megelőzés, a válaszintézkedések vagy a helyreállítási folyamatok terén. A dokumentum hasznos, de önmagában nem nyújt teljes körű támogatást.
  - A következő jellemzőkből többet is tartalmaz az adott dokumentum:
    - Alapvetések azonosítása a fenyegetésanalízissel kapcsolatban.
    - Felsőbb szintű meghatározása a megelőzési és védelmi stratégia kialakításának.
    - Általános követelmények leírását tartalmazza a válaszintézkedések kialakításával kapcsolatban.
    - Kevésbé részletes példák és esettanulmányok.
- Nem segít: a dokumentum nem nyújt megfelelő segítséget az adott fenyegetés kezelésében. Hiányoznak a releváns információk, a megelőzési stratégiák

és a válaszintézkedések. A dokumentum nem ad gyakorlati útmutatást, és nem járul hozzá hatékonyan a fenyegetés kezeléséhez.
– A következő jellemzőkből többet is tartalmaz az adott dokumentum:
  ° Hiányos vagy nem létező követelmények a fenyegetésanalízis témájában.
  ° Nincsenek vagy minimálisak a követelmények a megelőzési stratégiával kapcsolatban.
  ° Hiányzó vagy minimális követelmények a válaszintézkedésekkel kapcsolatban.
  ° Nincs gyakorlati példa vagy esettanulmány.

Ezek az értékelési kategóriák segítenek az egyes dokumentumok hatékonyságának meghatározásában és az okosrepülőterek számára releváns információk, anyagok kiválasztásában, hogy hatékonyan kezelhessék az adott fenyegetéseket.

2. táblázat: Részletes absztrakciós szinttel rendelkező dokumentumok vizsgálata az azonosított fenyegetések tükrében

Forrás-dokumentum	**Hálózati és kommunikációs támadás és DDoS-támadás**	**Rosszindulatú szoftver**	**Repülőtéri eszközök manipulációs támadásai**	**Engedéllyel való visszaélés támadása**	**Social engineering és adathalász-támadások**
Elsődleges, könnyen hozzáférhető szabályok az információbiztonságért[1]	Kielégítően segít	Kielégítően segít	Kielégítően segít	Kielégítően segít	Kielégítően segít
Okosrepülőterek biztonsága[2]	Kielégítően segít	Kielégítően segít	Kielégítően segít	Kielégítően segít	Kielégítően segít
A légi forgalmi irányítás kiberbiztonsági érettségi modellje[3]	Részben segít	Részben segít	Részben segít	Részben segít	Részben segít
Kiberbiztonsági kultúra a polgári repülésben[4]	Részben segít	Részben segít	Részben segít	Részben segít	Kielégítően segít

Forrás: a szerző szerkesztése

[1] EASA 2023.
[2] ENISA 2018.
[3] Eurocontrol 2019.
[4] ICAO 2022c.

Mindkét dokumentum, amely egészében lefedi az egyes kihívásokat, olyan részletes és átfogó kontrollkörnyezetet tartalmaz, amelyek együttes alkalmazása csökkenteni tudja az egyes fenyegetések kockázatát, mivel fő céljuk egy kockázatokkal arányos védelem kialakítása a szervezeten belül. Ezért ezen dokumentumok olyan információbiztonsági folyamatok kialakítását teszik lehetővé, amelyekkel az egyes összekapcsolt rendszerek sebezhetőségeit, az azokat kihasználó fenyegetéseket már a kezdetekkor azonosítják. Így fel lehet mérni, kezelni lehet, illetve folyamatosan figyelemmel lehet kísérni a fenti fenyegetések kockázatát.

A légi forgalmi irányítás kiberbiztonsági érettségi modellje dokumentum célja a kiberbiztonsági érettségi szint vizsgálata; hasznos és részletes dokumentum, de egy okosrepülőtér inkább csak a meglévő folyamatai értékelésére tudja használni, nem pedig azok kialakítására. Csak részben tud segítséget nyújtani az azonosított kihívásokkal szemben.

A *Kiberbiztonsági kultúra a polgári repülésben* dokumentum hatókörében megemlíti a kockázatok és fenyegetések csökkentésének támogatását. Illetve azokat a főbb alapelveket fejti ki, amelyek alapján működtetni kell az információbiztonságot. Részben tud segíteni az egyes fenyegetések elkerülésében vagy gyors felismerésében. A social engineering és adathalász-támadások esetében megtörtént a lefedés, mivel ezen dokumentum a személyi állománnyal foglalkozik, és részletesebben taglalja a tudatosítás és oktatás fontosságát.

A vizsgálatok igazolják H2 hipotézisemet: Az okosrepülőket érő kiberbiztonsági fenyegetésekre léteznek olyan nemzetközi dokumentációk, amelyek tudnak segíteni a létesítmények üzemeltetőinek, hogy felkészüljenek a kihívásokra, illetve azok hatékony elhárítására.

Összegzés

A cikk azonosítja, hogy pontosan mit is nevezhetünk okosrepülőtérnek, leírja a létesítmények főbb funkcióját és az azokat kiszolgáló rendszerelemeket. A rendszerelemek esetében látható volt a nagyobb fokú összekapcsolódás és az IoT-eszközök szerepe. Azonosítottuk azokat a fenyegetési kategóriákat, amelyekkel szembe kell néznie egy okosrepülőteret üzemeltető személyzetnek. A fenyegetéseket elemezve az látható, hogy az SoS-architektúra miatt egy rendszer sérülékenysége hatással van az egész összekapcsolt architektúrára. Ez alapján a fenyegetések mind *airside,* mind *landside* oldali rendszerekben megjelennek. A kutatás azon témakört is vizsgálta, hogy az USA, az EU és nemzetközi szervezetek viszonylatában milyen dokumentumok reflektálnak a légi közlekedés kiberbiztonságára. 28 dokumentumot azonosítottunk, amelyek jogszabályokat, ajánlásokat, stratégiákat tartalmaznak. Az elemzésből kiderült, hogy a kiberbiztonság milyen absztrakciós szinten jelenik meg ezen dokumentumokban. A legtöbb azonosított dokumentum alapszintű, ezt követik az átfogó publikációk, az érintőleges, valamint részletes leírások azonos megoszlást mutattak. Ha az Egyesült Államok és az Unió viszonylatában vizsgáljuk meg a kérdéskört, az látható, hogy utóbbi jóval több és részletesebb dokumentumot bocsátott ki. Megvizsgáltuk a dokumentumok használhatóságát az egyes azonosított fenyegetésekkel kapcsolatban.

Az elemzésből az látható, hogy vannak olyan publikációk, amelyek teljes mértékben segítséget tudnak nyújtani az azonosított fenyegetések kezelésére. Mindezt egy olyan információbiztonsági menedzsmentrendszer kialakításával, amelyben minden biztonsági eljárás, legyen az folyamatbéli, fizikai vagy technológiai, középpontjában a kockázatokkal arányos védelem áll. Tehát a fent azonosított fenyegetéstípusokat az okosrepülőtereknek a kezdetektől figyelembe kell venniük a működésük során, így azok bekövetkezési kockázatát alacsonyan tudják tartani.

A TKP2021-NVA-16 számú projekt a Technológiai és Ipari Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP2021-NVA pályázati program finanszírozásában valósult meg. A publikáció az I. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencia előadása alapján készült.

Felhasznált irodalom

AC 119-1A – Operational Authorization of Aircraft Network Security Program.

Alansari, Zainab – Soomro, Safeeullah – Belgaum, Mohammad Riyaz (2019): Smart Airports: Review and Open Research Issues. In Miraz, Mahdi H. et al. (szerk.): *Emerging Technologies in Computing*. International Publishing: Springer, 136–148. Online: http://dx.doi.org/10.1007/978-3-030-23943-5_10

AlMashari, Reema et al. (2018): *IoT-based Smart Airport Solution.* 2018 International Conference on Smart Communications and Networking, 1–6. Online: http://dx.doi.org/10.1109/SMARTNETS.2018.8707393

Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete (2018. július 4.) a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről.

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv).

Az Európai Parlament és a Tanács 376/2014/EU rendelete (2014. április 3.) a polgári légi közlekedési események jelentéséről, elemzéséről és nyomon követéséről, valamint a 996/2010/EU európai parlamenti és tanácsi rendelet módosításáról és a 2003/42/EK európai parlamenti és tanácsi irányelv, valamint az 1321/2007/EK bizottsági rendelet és az 1330/2007/EK bizottsági rendelet hatályon kívül helyezéséről EGT-vonatkozású szöveg.

A Bizottság (EU) 2015/1998 végrehajtási rendelete (2015. november 5.) a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról.

A Bizottság (EU) 2017/373 végrehajtási rendelete (2017. március 1.) a légiforgalmi szolgáltatást/léginavigációs szolgálatokat és más légiforgalmi szolgáltatási hálózati funkciókat és azok felügyeletét ellátó szolgáltatókra vonatkozó közös követelmények meghatározásáról, valamint a 482/2008/EK rendelet, az 1034/2011/EU, az 1035/2011/EU és az (EU) 2016/1377 végrehajtási rendelet hatályon kívül helyezéséről, továbbá a 677/2011/EU rendelet módosításáról.

A Bizottság (EU) 2019/1583 végrehajtási rendelete (2019. szeptember 25.) a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról szóló (EU) 2015/1998 végrehajtási rendeletnek a kiberbiztonsági intézkedések tekintetében történő módosításáról.

A Bizottság (EU) 2022/1645 felhatalmazáson alapuló rendelete (2022. július 14.) az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek a 748/2012/EU és a 139/2014/EU bizottsági rendelet hatálya alá tartozó szervezetekre vonatkozó, a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésével kapcsolatos követelmények tekintetében történő alkalmazására irányadó szabályok megállapításáról, valamint a 748/2012/EU és a 139/2014/EU bizottsági rendelet módosításáról.

A Bizottság (EU) 2023/203 végrehajtási rendelete (2022. október 27.) az (EU) 2018/1139 európai parlamenti és tanácsi rendeletnek az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU és az (EU) 2015/340 bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet hatálya alá tartozó szervezetek, valamint a 748/2012/EU, az 1321/2014/EU, a 965/2012/EU, az 1178/2011/EU, az (EU) 2015/340 és a 139/2014/EU bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet hatálya alá tartozó illetékes hatóságok tekintetében a repülésbiztonságra potenciálisan hatást gyakorló információbiztonsági kockázatok kezelésére vonatkozó követelmények tekintetében történő alkalmazására vonatkozó szabályok megállapításáról, valamint az 1178/2011/EU, a 748/2012/EU, a 965/2012/EU, a 139/2014/EU, az 1321/2014/EU és az (EU) 2015/340 bizottsági rendelet, továbbá az (EU) 2017/373 és az (EU) 2021/664 bizottsági végrehajtási rendelet módosításáról.

A Bizottság (EU) 2023/1769 végrehajtási rendelete (2023. szeptember 12.) a légiforgalmi szolgáltatási/léginavigációs szolgálati rendszerek és rendszerelemek tervezésében vagy gyártásában részt vevő szervezetek jóváhagyására vonatkozó műszaki követelmények és igazgatási eljárások meghatározásáról, valamint az (EU) 2023/203 végrehajtási rendelet módosításáról.

Bestugin, A. R. et al. (2020): Advanced Automated ATC Systems. In *Air Traffic Control Automated Systems.* Singapore: Springer, 25–123. Online: https://doi.org/10.1007/978-981-13-9386-0_2

Blondel, Mathieu – Zintel, Michael – Suzuki, Hiroto (2015): *Airports 4.0: Impact of Digital Transformation on Airport Economics.* Online: www.adlittle.com/sites/default/files/viewpoints/2015-05-Arthur_D_Little_T_T-Impact_of_Digital_on_Airport_Business_Model.pdf

CANSO (2020): *CANSO Standard of Excellence in Cybersecurity.* Online: https://canso.fra1.digitaloceanspaces.com/uploads/2021/04/canso_standard_of_excellence_in_cybersecurity.pdf

CANSO (2021): *Air Traffic Management Cybersecurity Policy Template.* Online: https://canso.fra1.digitaloceanspaces.com/uploads/2021/04/air_traffic_management_cybersecurity_policy_template-EN.pdf
CISA (2015): *Transportation Systems Sector-Specific Plan – 2015.* Online: www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems
EASA (2023): *First Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645).* Online: www.easa.europa.eu/en/document-library/easy-access-rules/first-easy-access-rules-information-security-regulations-eu
ENISA (2018): *Securing Smart Airports. Available.* Online: www.enisa.europa.eu/publications/securing-smart-airports
Euorcontrol (2019): *ATM Cybersecurity Maturity Model Level 1.* Online: www.eurocontrol.int/sites/default/files/2019-09/atm-cybersecurity-maturity-model.pdf
FAA (2020): *Cybersecurity Strategy.* Online: www.faa.gov/sites/faa.gov/files/FAA_Cybersecurity_Strategy_PL_115-254_Sec509.pdf
FATTAH, Amir et al. (2009): *Smart Airports: Transforming Passenger Experience To Thrive in the New Economy.* Cisco Internet Business Solutions Group (IBSG). Online: www.cisco.com/c/dam/en_us/about/ac79/docs/pov/Passenger_Exp_POV_0720aFINAL.pdf
HÄTTENSCHWILER, Nicole et al. (2018): Automation in Airport Security X-Ray Screening of Cabin Baggage: Examining Benefits and Possible Implementations of Automated Explosives Detection. *Applied Ergonomics, 72*, 58–68. Online: https://doi.org/10.1016/j.apergo.2018.05.003
H.R.302 – An act to provide protections for certain sports medicine professionals, to reauthorize Federal aviation programs, to improve aircraft safety certification processes, and for other purposes
IATA (2021): *Aviation Cyber Security Guidance Material Form.* Online: www.iata.org/en/programs/security/cyber-security/aviation-cyber-security-guidance-form/
IATA (2024): *Security Management System Manual (SeMS).* Online: www.iata.org/en/publications/store/security-management-system-manual/
ICAO (2019): *Aviation Cybersecurity Strategy.* Online: www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx
ICAO (2022a): *Presentation of 2022 Air Transport Statistical Results.* Online: www.icao.int/sustainability/WorldofAirTransport/Documents/ARC_2022_Tables_final_12032024.pdf
ICAO (2022b): *Cybersecurity Action Plan.* Online: www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx
ICAO (2022c): *Cybersecurity Culture in Civil Aviation.* Online: www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Culture%20in%20Civil%20Aviation.EN.pdf
ICAO (2022d): *Cybersecurity Policy Guidance.* Online: www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf
ICAO (2022e): *Guidance on Traffic Light Protocol.* Online: www.icao.int/aviationcybersecurity/Documents/Guidance%20on%20Traffic%20Light%20Protocol%20Policy.EN.pdf

Lykou, Georgia – Anagnostopoulou, Argiro – Gritzalis, Dimitris (2018): Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors,* 19(1), 19. Online: https://doi.org/10.3390/s19010019

Mantouka, Eleni et al. (2018): Gamification in Mobile Applications: The Case of Airports. *Journal of Intelligent Transportation Systems,* 23(5), 1–10. Online: https://doi.org/10.1080/15472450.2018.1473157

Marks, Adam – Rietsema, Kees (2014): Airport Information Systems—Airside Management Information Systems. *Intelligent Information Management,* 6(3), 149–156. Online: https://doi.org/10.4236/iim.2014.63016

Nau, Jean Baptiste – Benoit, Franck (2017): *Smart Airport: How Technology is Shaping the Future of Airports.* Online: https://wwa.wavestone.com/app/uploads/2017/12/Smart-Airport-2017.pdf

Presidential Policy Directive/PPD-21 – Critical Infrastructure Security and Resilience.

Rajapaksha, Aruna – Jayasuriya, Nisha (2020): Smart Airport: A Review on Future of the Airport Operation. *Global Journal of Management and Business Research,* 20(3), 25–34. Online: https://doi.org/10.34257/GJMBRAVOL20IS3PG25

del Río, José Sánchez et al. (2016): Automated Border Control E-Gates and Facial Recognition Systems. *Computers & Security,* 62, 49–72. Online: https://doi.org/10.1016/j.cose.2016.07.001

Sharkov, George (2017): A System-of-Systems Approach to Cyber Security and Resilience. *Information & Security,* 37, 69–94. Online: https://doi.org/10.11610/isij.3706

SITA (2023): *Air Transport IT Insights 2023.* Online: www.sita.aero/resources/surveys-reports/air-transport-it-insights-2023/

Tabares, Diego – Mora-Camino, Felix (2019): Aircraft Ground Operations: Steps Towards Automation. *CEAS Aeronautical Journal,* 10(3), 965–974. Online: https://doi.org/10.1007/s13272-019-00390-5

TSA (2018): *TSA Cybersecurity Roadmap.* Online: www.tsa.gov/sites/default/files/tsa_cybersecurity_roadmap.pdf

Wang, Le (2018): Application of Wireless Sensor Network and RFID Monitoring System in Airport Logistics. *International Journal of Online and Biomedical Engineering (iJOE),* 14(1), 89–103. Online: https://doi.org/10.3991/ijoe.v14i01.8058

Wittmer, Andreas (2011): Acceptance of Self-service Check-in at Zurich Airport. *Research in Transportation Business & Management,* 1(1), 136–143. Online: https://doi.org/10.1016/j.rtbm.2011.06.001

Yang, Shen (2010): *Architecture of Airport Operation Database System.* 2009 First International Conference on Information Science and Engineering, 2278–2281. Online: https://doi.org/10.1109/ICISE.2009.346