REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK
32. évfolyam (2020) 2. szám 165–180. • DOI: 10.32560/rk.2020.2.12

Peredy Zoltán,[1] Venczel Márk[2]

Nemzetközi repülőterek kiberbiztonsági kihívásai

Az elmúlt néhány évben a nemzetközi repülőterek földi és légi infrastruktúrájának működtetése egyre bonyolultabb technológiákat, automatizált rendszereket követelt, amely megnövelte a repülőterek és a légi közlekedési ágazat sérülékenységét a számítógépes bűnözőkkel és terroristákkal szemben. A Covid-19-járvány még tovább súlyosbította a helyzetet. A repülőterek és a légi járművek elleni kibertámadások lehetősége valódi veszélyeket rejt magában, úgymint a földi és légi infrastruktúrák folyamatos és zökkenőmentes működtetésének akadályozása; az üzembiztonság sérülése; az adatok illetéktelen kezekbe való kerülése vagy az informatikai és kommunikációs rendszerek összeomlása. Jelen áttekintő cikk célja, hogy összegezze a nagy nemzetközi repülőterek elleni kibertámadások főbb okait, típusait, hatásait, kockázatait és ezek minimalizálásának lehetőségeit néhány konkrét nemzetközi példa bemutatásával. Ezen túlmenően javaslatokat fogalmaz meg a kibertámadásoknak való kitettség csökkentésére szervezeti, működési megoldásokkal, úgymint információk megosztása, kibertudatosság növelése, valamint a hálózatos együttműködések kialakítása.

Kulcsszavak: *kiberbiztonság, kiberterrorizmus, IKT-rendszer, védett adat elvesztése, intelligens repülőtér*

Cybersecurity Challenges at International Airports

Over the past few years, the operation of ground and air infrastructure at international airports has required increasingly sophisticated technologies and automated systems, which have increased the vulnerability of airports and the aviation sector to cyber criminals and terrorists. The situation has been exacerbated by the Covid-19 epidemic. The possibility of cyberattacks against airports and aircraft poses real dangers such as the obstruction of continuous and smooth operation of ground and air infrastructures, serious breaches of operational security, loss of data and its acquirement by unauthorised hands, collapse of IoT and communication systems. The aim of this review article is to provide relevant and up-to-date landscape related to the main causes, types, impacts, risks and minimisation of cyberattacks against large international airports by presenting some concrete international examples, and to make proposals to reduce exposure

[1] Edutus Egyetem Műszaki Intézet, intézetvezető, e-mail: peredy.zoltan@edutus.hu, ORCID: https://orcid.org/0000-0002-4074-8430
[2] Budapesti Műszaki és Gazdaságtudományi Egyetem Közlekedésmérnöki és Járműmérnöki Kar Vasúti Járművek, Repülőgépek és Hajók Tanszék, doktori hallgató, e-mail: mvenczel@vrht.bme.hu, ORCID: https://orcid.org/0000-0002-4319-1463

to cyberattacks through organisational and operational solutions such as information sharing, cyber awareness and networking.

Keywords: *cybersecurity, cyberterrorism, ICT system, data breach, smart airport*

1. Bevezetés

A Covid-19 koronavírus-járvány a Nemzetközi Valutaalap és a Világbank szakértőinek számításai szerint 2020-ban a világ GDP-jében 3–5,2%-os visszaesést fog előreláthatóan okozni, felülmúlva a 2008–2009. évi globális pénzügyi-gazdasági válság mértékét.[3] A sokszereplős, nagy beszállítói láncoktól való függés és a leállásuk okozta tovagyűrűző hatások több ágazatot hoztak nehéz helyzetbe, köztük a légi közlekedési iparágat is. A járvány negatívan befolyásolta a nemzetközi utasforgalom és légi teherszállítás alakulását, valamint a repülőterek működését és az iparág jövedelemtermelő képességét. A 2019. évi adatokkal való összevetés alapján a korábbi 4,72 milliárd fő globális (nemzetközi és belföldi) utasforgalom 45–60%-kal csökken (2020-ban a járványt követően 2,2 milliárd fő, míg 2021-ben is csak 3,38 milliárd fő valószínűsíthető), miközben a repülőjáratok helykihasználtsága 40–53%-kal esett vissza (számos járat teljesen le is állt), a légitársaságok pedig 300–400 milliárd dollár működési veszteséget realizáltak a járvány időtartama alatt.[4]

Az elmúlt néhány évben a nemzetközi repülőterek földi és légi infrastruktúrájának működtetése egyre bonyolultabb technológiákat, automatizált rendszereket követelt, amely megnövelte a repülőterek és a légi közlekedési ágazat sérülékenységét a számítógépes bűnözőkkel és terroristákkal, valamint azon bennfentes alkalmazottakkal szemben, akik az adatok ellopásával, a kritikus infrastruktúrák működési biztonságának akadályozásával zavart, bizonytalanságot, fennakadásokat kívánnak kelteni, amely állapotokat a járvány okozta helyzet még tovább súlyosbított.

A légi közlekedési ágazat informatikai beruházásainak szintje 2014–2019 között 21,4 milliárd dollárról 35,2 milliárd dollárra növekedett. A teljes IKT- (Információs és Kommunikációs Technológia) beruházásokon belül a kiberbiztonság növelését célzó fejlesztések aránya 2016-ban 4,6%; 2017-ben 7%; 2018-ban 9% és 2019-ben 14% volt.[5] A repülőterek kiberfenyegetettségekkel szembeni ellenállásának javítása azonban nem kizárólag a pénzügyi forrásokon múlik, ehhez az egyes repülőterek kiberbiztonsági érettségi szintjét is növelni szükséges. Ezen szemléletváltáshoz a járvány utóhatásai valószínűleg hozzá fognak járulni. Szükségeltetik egy tudatos kiberbiztonsági politika megfogalmazása a kockázatok rendszeres feltérképezésével és beazonosításával; információk, kiberbiztonsági incidensek, tapasztalatok, tanulságok, legjobb gyakorlatok kölcsönös megosztása; valamint a hálózatos együttműködés kiépítése és megfelelő szabályozási környezet kialakítása a munkavállalók érzékenyítésével és a kiberbiztonsági tudatossági szint képzésekkel, tréningekkel történő emelésével.[6]

Jelen publikáció célja, hogy áttekintse a nagy nemzetközi repülőterek elleni kibertámadások főbb okait, típusait, hatásait, kockázatait és ezek minimalizálásának lehetőségeit

[3] *Effects of Novel Coronavirus (COVID-19) on Civil Aviation: Economic Impact Analysis.* ICAO, 2020. 12.
[4] E. Mazareanu: *Coronavirus: impact on the aviation industry worldwide.* Statista, 4 Jun 2020. 1.
[5] R. Florent: *Aerospace Cybersecurity: Building resilience in the hailstorm.* Cyber Inflight, 10 May 2020. 1.
[6] *Security and Facilitation Strategic Objective. Aviation Cybersecurity Strategy.* ICAO, 2019. 3–4.; *A40-10: Addressing Cybersecurity in Civil Aviation.* ICAO, 2019. 1–2.

néhány konkrét nemzetközi példa bemutatásával. A nemzetközi áttekintés a szekunder vagy „desk research" kutatási módszerekre támaszkodik, amelynek eszköze a meglévő releváns hazai, európai uniós, valamint a WEF[7]-, IATA[8]- és ICAO[9]-dokumentumok, publikációk, online weboldalak áttekintése, majd az így összegyűjtött adatok rendszerezése, szelektálása, elemzése. Emellett primer információk felhasználásával (munkamegbeszélések alapján) készült a jelen tanulmány. A nemzetközi tapasztalatokra épülő, a konkrét példákra vonatkozó elemzésből levont főbb következtetések, tanulságok a szerzők saját szakmai véleményét tükrözik.

2. Nemzetközi repülőterek kiberfenyegetéseinek kérdései

2.1. Repülőterek kategorizálása az IKT és az okos alkalmazások szemszögéből

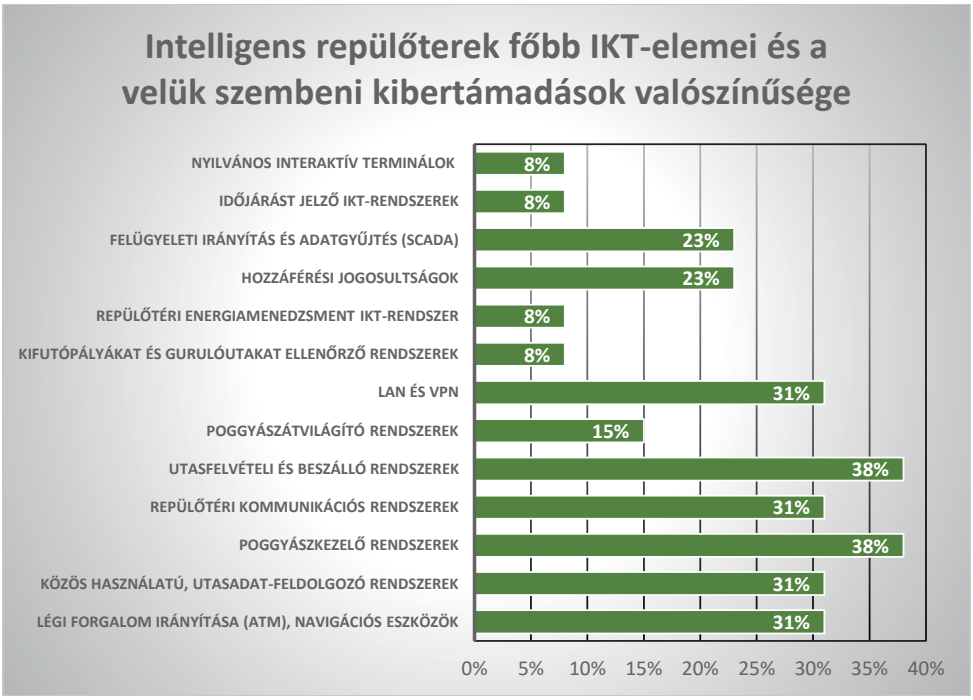
A repülőterek az IKT és az intelligens alkalmazások révén javították interoperabilitási képességeiket a hatékonyság elérése érdekében, ezért a kritikus infrastruktúrák összetettsége jelentős mértékben megnőtt. A nemzetközi repülőterek IKT-alapú működési megoldásaik szerint az alábbi három kategória valamelyikébe sorolhatók be:[10]

- *hagyományos repülőterek,* amelyek a leszállások, indulások és egyéb légi járművek biztonságos és hatékony kezeléséhez szükséges képességekre összpontosítanak, alapszintű személyszállítási szolgáltatások nyújtásával;
- *agilis repülőterek,* amelyek alkalmazkodnak a változó digitális környezethez azáltal, hogy „testre szabott" szolgáltatásokat kínálnak egy közös platformon;
- *intelligens repülőterek,* amelyek teljes mértékben kihasználják az IoT[11]- és a digitalizációs technológiák lehetőségeit, és átfogóan kombinálják azokat a biztonsági elemekkel. A valós idejű információcsere, a széles körű együttműködés és a repülőtéri folyamatok integrációjának köszönhetően az intelligens repülőterek jelentősen javítják a működési hatékonyságukat, az utasszolgáltatás színvonalát és a kiberbiztonsági szintjüket.[12]

Az ENISA[13] szerint az intelligens repülőterek azok, amelyek hálózatba kötött, adatközpontú válaszadási képességeket használnak egyrészt a jobb utazási élmény nyújtása, másrészt pedig az utasok biztonságának magasabb szintű garantálása érdekében.[14] Mivel a repülés szempontjából a biztonság és védelem a legfontosabb területek, a biztonságos környezetet összetett kiberbiztonsági kihívások proaktív kezelésével kell biztosítani, miközben minimalizálni kell a működési műveletek fennakadását, zavarát. Az 1. ábra nyolc ország 20 repülőterén

7 WEF: World Economic Forum – Világgazdasági Fórum.
8 IATA: International Air Transport Association – Nemzetközi Légi Szállítási Szövetség.
9 ICAO: International Civil Aviation Organisation – Nemzetközi Polgári Repülési Szervezet.
10 Georgia Lykou – Argiro Anagnostopoulou – Dimitris Gritzalis: Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors,* 19. (2019), 1. 4.
11 IoT: Internet of Things – dolgok internete, más szavakkal hálózatba kötött intelligens eszközök gyűjtőneve.
12 R. Pethuru – A. C. Raman: *The Internet of Things. Enabling Technologies, Platforms & Use Cases.* CRC Press, Taylor&Francis Group, 2017. 256–257.
13 ENISA: European Union Agency for Cybersecurity – Európai Uniós Kiberbiztonsági Ügynökség.
14 Lykou–Anagnostopoulou–Gritzalis (2019) i. m. 4.

végzett felmérés alapján összegzi a repülőtéri IKT-infrastruktúra kritikus elemeit és azt, hogy milyen gyakorisággal szolgálhatnak a kibertámadások célpontjaiként.



1. ábra
A nemzetközi repülőterek IKT-vagyonelemeinek kibertámadás szempontjából kritikus részei. Forrás: *Securing Smart Airports.* ENISA, Study, 2016. 24. alapján a szerzők saját szerkesztése

2.2. Kibertámadások fajtái

A nemzetközi repülőtereken egyre inkább előtérbe kerül a digitális technológiák széles körű használata. A kibertér (cyberspace) is szolgálhat a légi közlekedés elleni terrortámadások végrehajtásának platformjaként. A repülőterek és a légi járművek elleni kibertámadások lehetősége valódi veszélyeket rejt magában, úgymint a földi és légi infrastruktúrák folyamatos és zökkenőmentes működtetésének akadályozása, az üzembiztonság sérülése, adatok illetéktelen kezekbe való kerülése, valamint az informatikai és kommunikációs rendszerek összeomlása által.[15] Az 1. táblázat összefoglalja a repülőterek elleni kibertámadások főbb típusait, negatív hatásait, valamint ezen hatások minimalizálását lehetővé tevő javasolt intézkedéseket.

[15] Eitan Azani – Lorena Atiyas Lvovsky – Danielle Haberfeld: *Trends in Aviation Terrorism.* International Institute for Counter-Terrorism (ICT), 2016. 13–14.

1. táblázat
A nemzetközi repülőterek főbb kiberbiztonsági kihívásai és az azokra adandó lehetséges válaszok. Forrás: Lykou–Anagnostopoulou–Gritzalis (2019) 8–9.; *Securing Smart Airports.* (2016) i. m. 26–29. alapján a szerzők saját szerkesztése

Kibertámadás típusa	Érintett területek	Negatív hatások	Hatások minimalizálásának lehetőségei
Túlterheléses támadás[16] (DoS)	• Webszolgáltatások • ATM-kommunikációk • Mobiltelefon-hálózat • Vezeték nélküli kommunikáció	• Földi és légi infrastruktúrát érintő műveletek akadályozása • Repülőtéri interoperabilitás akadályozása	• Vészhelyzeti protokollokra forgatókönyv • A repülőtér működésével és üzembiztonságával kapcsolatos anomáliák kommunikálása az érintettek felé • Tűzfalak, hálózati szegmentálás, illetéktelen behatolás elleni védelem
Kommunikációs támadás	• Légi forgalom irányítása • Repülőgépek navigációs és GPS-rendszerei[17]	• Repülőtér-működtetés és az üzembiztonság veszélyeztetése • Légi járművek biztonságának veszélyeztetése	• Alternatív üzemeltetési megoldások • Incidensekre való azonnali reagálás képessége • Biztonságos kommunikációs csatornák • Adatok titkosítása, hamisítás elleni küzdelem
Ártó szándékú szoftverek	• Számítógépes hálózatok • Szerverek • Légi utasok és a repülőtéri alkalmazottak „okos" informatikai eszközei	• Informatikai és kommunikációs rendszerek működésének akadályozása • Földi és légi műveletek akadályozása	• Hatékony vírusvédelem • Informatikai incidensekre való azonnali reagálás • Információbiztonsági tudatosság növelése, munkavállalók érzékenyítése tréningekkel • Rendszeres szoftver- és hardverkarbantartás • Kiberbiztonsági protokollok • Előre jelző és elemző kapacitások kiépítése

[16] A szolgáltatásmegtagadással járó támadás (Denial of Service, DoS), más néven túlterheléses támadás, informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. A szolgáltatásmegtagadás-támadás egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeire vagy valamilyen speciális protokoll tulajdonságaira fókuszál. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógéprendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. (*Understanding Denial-of-Service Attacks.* Cybersecurity and Infrastructure Security Agency, 20 November 2019. 1.)

[17] Kiberbiztonsági szakértők szerint a hackerek képesek feltörni a repülőgép vezérlőrendszerét az utasülésükből megzavarva a repülőgép GPS- és navigációs rendszereit. A pilótafülke hálózatába a repülőgép hálózatával való kommunikáció útján lehetséges bejutni. (A repülőgépek fedélzetén sok elektronikai szórakoztató rendszer USB-csatlakozással rendelkezik, és több légitársaság wifit is üzemeltet a járatain, amelyeknek kommunikációs hálózati architektúrája nem megfelelő, mivel vannak olyan biztonsági rések, amelyek lehetővé teszik a repülési rendszerekbe való illetéktelen belépést is.) (Anthony Lam – Jose Fernandez – Richard Frank: Cyberterrorists Bringing Down Airplanes: Will it Happen Soon? In A. R. Bryton – J. R. Lopez Jr. – R. F. Mills: *Academic Conferences and Publishing International Limited Reading.* Proceedings of 12th International Conference on Cyber Warfare and Security, Wright State University with the Air Force Institute of Technology Dayton, UK, 2–3 March 2017. 210–219.)

Kibertámadás típusa	Érintett területek	Negatív hatások	Hatások minimalizálásának lehetőségei
Hálózati támadás	Zárt kamerás rendszerek (CCTV) ICS SCADA-rendszerek[18] Csomagkezelés Földi infrastruktúra-műveletek	Földi és légi infrastruktúra működtetésének és a létesítmény-menedzsmentnek az akadályozása	• Előre jelző és kockázatelemző kapacitások kiépítése, működtetése • Incidensekre való azonnali reagálás képessége • Vészhelyzeti protokollok működtetése • Biztonsági tudatosság növelése tréningekkel • Adatok titkosítása • Hozzáférési szintek és jogosultságok szabályozása • Informatikai eszközök hitelesítése
Felhatalmazással való visszaélés	ICS SCADA-rendszerek Repülőtéri infrastruktúrákba/ terminálokra való belépések ellenőrzése Légi forgalom irányítása	Földi és légi infrastruktúra működtetésének és a létesítmény-menedzsmentnek az akadályozása	• Előre jelző és kockázatelemző kapacitások kiépítése, működtetése • Incidensekre való azonnali reagálás képessége • Vészhelyzeti protokollok működtetése • Biztonsági tudatosság növelése tréningekkel • Repülőtéri alkalmazottak megfelelő kiválasztása (HR-politika) • Adatok titkosítása • Hozzáférési szintek és jogosultságok szabályozása
Adathalászat	ICS SCADA-rendszerek IT és kommunikációs rendszerek Földi infrastruktúra	Repülőtéri adminisztráció munkavégzésének, a földi és légi infrastruktúra működtetésének és a létesítmény-menedzsmentnek az akadályozása	• IT biztonsági kultúra megteremtése • Etikai szabályok • Alkalmazottak ösztönzése „Gondolkodj, mielőtt kattintasz” • Erős felhasználói hitelesítés • Tűzfalak, hálózatok szegmentálása • Behatolások felderítése • Szoftverek és hardverek karbantartása

A számítógépes támadások végrehajtásához professzionális felkészültségű hackerekre van szükség, ezért a terroristaszervezeteknek egyik kiemelt céljuk, hogy soraikba ilyen „szakemberek” beszervezésével a kibertérben is működni tudjanak. Ennek ellenére a szakértők becslései szerint a terroristaszervezetek egyelőre nem képesek jelentős társadalmi-gazdasági hatással járó kibertámadásokat végrehajtani a polgári repülőgépek vagy a nagy nemzetközi repülőterek ellen.[19]

[18] Ipari ellenőrző rendszer (Industrial Control System, ICS) a különböző ipari/értékteremtő folyamatokat felügyelő és irányító informatikai rendszer (például automatizált gyártósorok felügyeletét, épületek energiafelhasználásának mérését vagy biztonsági felügyeletét végző informatikai megoldások). Az ICS-eket gyakran programozható logikai vezérlőkön (Programmable Logic Controller, PLC) vagy felügyeleti adatgyűjtő és ellenőrző rendszereken (Supervisory Control and Data Acquisition, SCADA) keresztül működtetik. Ez utóbbi biztosítja az operátor számára az adatok grafikus megjelenítését a szükséges beavatkozások meghatározása érdekében. [Keith Stouffer – Joe Falco – Karen Scarfone: *Guide to Industrial Control Systems (ICS) Security.* Recommendations of the National Institute of Standards and Technology, U.S. Department of Commerce, 2011. 16.]

[19] Azani–Lvovsky–Haberfeld (2016) i. m. 15.

A repülőtéri infrastruktúrák és a légi közlekedés elleni kibertámadások főbb mozgatórugói:[20]

- *Politikai vagy katonai okok:* A külföldi katonai vagy hírszerzési források célja, hogy az adott ország gazdasági, politikai rendszerének, integritásának és a közbizalom befolyásolására alkalmas stratégiai információkat szerezzenek meg. A repülőterek vonzó célpontjai a kibertámadásoknak, hiszen bármilyen zavar befolyásolhatja a légi közlekedésbe vetett bizalmat és a nemzeti légtér biztonságát.
- *Ipari/kereskedelmi kémkedés:* Az ilyen motivációval rendelkező támadók célja a versenytársaikkal kapcsolatos bizalmas vagy védett információk ellopása vagy kiszivárogtatása csalás, zsarolás, pénzügyi haszonszerzés vagy vállalati stratégiai előnyök megszerzése érdekében. Ilyen jellegű tevékenység célja például a repülőterek adminisztrációs dokumentumainak (ideértve a tervezési, építési, költségvetési, pénzügyi, jogi és kormányzati dokumentumokat) megszerzése.
- *Civil szervezetek zavarkeltési akciói:* A különböző aktivisták, tiltakozók célja, hogy megzavarják vagy letiltsák az erőforrásokhoz való hozzáférést, annak érdekében, hogy helyzetükre vagy az általuk képviselt álláspontra ráirányítsák a nyilvánosság figyelmét. Tipikus példa a szolgáltatásmegtagadási támadások (DoS) a repülőtér környezetében, ahol a támadók arra törekszenek, hogy megakadályozzák a repülőtér weboldalához való hozzáférést, vagy megzavarják az online szolgáltatásokat.
- *Számítógépes bűnözés:* A támadók általában közvetlenül a különböző hálózatokat és informatikai rendszereket célozzák meg, hogy ellopják és értékesítsék az adatokat (például az ügyfél azonosítását, hitelkártyáját vagy banki adatait). Manapság ez a támadások egyik leggyorsabban növekvő területe. E támadók elsődleges célpontjai lehetnek azok a repülőterek, amelyek hitelkártya-információkat kezelnek fizetési szolgáltatásokért (például poggyászdíjak vagy parkolási díjak). Noha ezek a támadások kevésbé kifinomultak, mint a többi típus, a számítógépes bűnözés technikái az utóbbi időkben jelentős mértékben fejlődtek. Például zsarolóprogramok használatával a támadók képesek titkosítani az adatokat, és utána azzal fenyegetik áldozataikat, hogyha nem fizetnek a titkosítás feloldása érdekében egy megadott összeget, akkor ezeket az adatokat kiszivárogtatják vagy megsemmisítik.

2.3. Kibertámadások főbb kockázatai

A repülőterek kritikus infrastruktúrái ellen elkövetett különböző kibertámadások fajtái és azok negatív hatásainak elemzése mellett célszerű megvizsgálni a kibertámadások által jelentett főbb kockázatokat is. A repülőterek informatikai és technológiai infrastruktúrájának kibertámadásokkal szembeni sérülékenysége globális rendszerszintű biztonsági kockázatokat jelent. A 2. táblázat összefoglalja az öt legfontosabb Közlekedési Kockázati Indexet, és ezek súlyát a légi közlekedés és a repülőterek vonatkozásában.

[20] Lykou–Anagnostopoulou–Gritzalis (2019) i. m. 20.

2. táblázat
Közlekedési Kockázati Indexek és súlyuk. Forrás: *Advancing Cyber Resilience in Aviation: An Industry Analysis.* World Economic Forum, 2020. 10. alapján a szerzők saját szerkesztése

Rang-sor	Közlekedési szektor	Levegő (repüléstámogató infrastruktúra a talajtól a világűrig)	Repülőterek
1.	Megnövekedett biztonsági fenyegetések a kibertér és az adatvédelem megsértői részéről	Kritikus informatikai rendszerek összeomlása	Versenyjogi monitorozás/ cégek egyesülésével létrejövő monopóliumok létrejöttének megakadályozása
2.	Kritikus informatikai rendszerek összeomlása	Versenyjogi monitorozás/ cégek egyesülésével létrejövő monopóliumok létrejöttének megakadályozása	A szezonális kereslet változása, amely a szállítás hiányához vagy túlkínálatához vezet (a kihasználtság / az árakat befolyásoló kapacitás)
3.	Harmadik (beszállító) féltől való függés	Harmadik (beszállító) féltől való függés	Kritikus informatikai rendszerek összeomlása
4.	Harmadik fél biztonsági sérülékenysége, digitális ellátási lánc ellenálló képessége	A technológiai fejlődéssel vagy a változásokkal való lépéstartás képtelensége	Extrém időjárási események/ természeti katasztrófák, fegyveres konfliktusok, járványok
5.	Versenyjogi monitorozás/ cégek egyesülésével létrejövő monopóliumok létrejöttének megakadályozása	Nemzeti infrastruktúráktól való túlzott függőség	Megnövekedett biztonsági fenyegetések a kibertér és az adatvédelem megsértői részéről

A 2. táblázatban szereplő kiberkockázatok és azok következményei egyre szélesebb körűvé válnak, amelyek a légi közlekedési ágazat minden területén érzékelhető veszteségeket, fennakadásokat okoztak az elmúlt években. Ezért alapvető, hogy a repülőipar érintett szereplői kidolgozzanak és összehangolják kiberellenálló képességüket növelő stratégiákat ezen hatások enyhítésére és a kritikus infrastruktúrák védelmére, ahogy az a 2019-es ICAO-jelentésben[21] is szerepel.

2.4. Nemzetközi példák a különböző kibertámadásokra és azok hatásaira

Érdemes áttekinteni hat jelentős nemzetközi repülőtér/légitársaság olyan információbiztonsági incidenseit, amely utasok ezreinek az élet- és vagyonbiztonságát fenyegethette volna.

2.4.1. Heathrow repülőtér: védett adatok elvesztéséért pénzbírság kiszabása

Az ICO[22] 120 000 fontra bírságolta a Heathrow Nemzetközi Repülőteret azért, mert nem tette meg a szükséges megelőző információbiztonsági intézkedéseket. Erre akkor derült fény, miután egy alkalmazott 2017 októberében elvesztett egy bizalmas információkat tartalmazó memóriakártyát, amelyet egy utas talált meg, és annak tartalmát egy nyugat-londoni könyvtárban megnézte. A memóriakártya olyan érzékeny adatokat tartalmazott, mint a királynő

[21] *Aviation Cyber Security – Moving Forwards.* IATA, ICAO Working Paper on Assembly 40th Session Executive Committee, 2019. 1.
[22] ICO: Information Commissioner's Office – brit Adatvédelmi Hivatal.

és a kormánytagok utazási útvonalai és azok időpontjai, vagy 50 alkalmazott teljes körű személyes adatait, akik a repülőtéri biztonságért feleltek. Az adatok nem voltak titkosítva, sem jelszóval védve. Az ICO vizsgálata alapján kiderült az is, hogy a Heathrow repülőtér 6 500 fő munkavállalója közül összesen 2% részesült adatvédelmi és információbiztonsági képzésben, így a repülőteret ezen hiányosság pótlására is kötelezték.[23]

2.4.2. Atlanta repülőtér: zsarolóprogram által kikényszerített wifileállás

Hartsfield–Jackson Atlanta Nemzetközi Repülőtér 2018 márciusában leállította a wifi hálózatának működtetését, miután Atlanta város önkormányzatának internetes hálózata zsarolóvírus-támadásnak esett áldozatul. A hivatali számítógépeken található file-okat egy Sam-Sam néven ismert támadó titkosította, és váltságdíjat követelt azok dekódolásáért. A repülőtér kikapcsolta a wifi-szolgáltatását, hogy elkerülje a rosszindulatú zsarolóprogramok terjedését a repülőtéri hatóságok, a légitársaságok és az ügyfelek számítógépein. Az incidens nem okozott fennakadást a légi forgalomban.[24]

2.4.3. British Airways: tömeges adatlopás

2018 augusztusában a British Airways 38 000 utasának személyes és pénzügyi adatait (nevek, bankszámlaszámok, hitelkártyaadatok, lejárati dátumok, háromjegyű CVV-kódok és e-mail-címek) lopták el ismeretlen hackerek. A BA weboldalára feltett üzenet szerint az ügyfeleknek kapcsolatba kell lépniük bankjaikkal, bármilyen ismeretlen, nem jóváhagyott tranzakció vagy adataikkal való visszaélés esetén.[25]

2.4.4. Cathay Pacific: személyes adatok millióinak kiszivárogtatása

A hongkongi légitársaság példátlan kockázatnak tette ki közel 9,4 millió ügyfelét 2018 márciusában, miután személyes adataikhoz (személyiigazolvány- vagy útlevélszámok, e-mail-címek, hitelkártyaadatok, utazási előzmények) illetéktelenek hozzáférést szereztek az információbiztonsági rendszerek hézagait kihasználva. A légitársaság azonnali vizsgálatot indított, hogy kiderítse, ki áll a kibertámadás mögött, illetve szigorítottak az információbiztonsági intézkedéseken.[26]

[23] Varsha Saraogi: *Five times airports were involved in cyberattacks and data breaches.* Airport Technology, 24 July 2019. 1.
[24] Uo. 1.
[25] Uo. 1.
[26] Uo. 1.

2.4.5. Air Canada: privát információkat loptak el mobilapplikáción keresztül

Az Air Canada légitársaság 2018 augusztusában egy olyan szokatlan, illetéktelen bejelentkezést/behatolási kísérletet észlelt, amelyen keresztül az ügyfelek személyes adataihoz próbáltak meg hozzáférni. A légitársaság azonnal zárolta 1,7 millió utasának számláit és adatait, de így is megkéstek az intézkedéssel: 20 000 ügyfél adatait (nevek, e-mail-címek, telefonszámok, útlevéladatok) ellopták.[27]

2.4.6. LOT: üzemképtelenné tett számítógépes repülőjegy-foglalási és -kiadási rendszer

2015 júniusában Varsóban a lengyel nemzeti légitársaság (LOT) számítógépes foglalási és repülőjegy-kiadási rendszerét érte hackertámadás, azt üzemképtelenné téve és egyben tucatnyi járat késését vagy törlését okozva.[28]

3. Egy érdekes nemzetközi kiberbiztonsági felmérés eredményei

Az ImmuniWeb nevű kiberbiztonsági cég több szempontra kiterjedő felmérést[29] végzett a világ 100 különböző, jelentős nemzetközi repülőterén a kibertámadásokkal szembeni biztonságosság elemzése érdekében. Az eredmények alapján kiberbiztonsági szempontból az alábbi három repülőtér bizonyult a legbiztonságosabbnak:

- amszterdami repülőtér, Schiphol (EU);
- Helsinki-Vantaan repülőtér (EU);
- dublini repülőtér (EU).

Míg a maradék 97 vizsgált repülőtér IKT-rendszere valahol sérülékenynek mutatkozott a felmérésből. A kiberbiztonsági vizsgálat a következő alfejezetekben részletezett szempontok alapján történt.

3.1. Repülőterek hivatalos weboldalainak biztonsága

A számítógépes bűnözők külső támadásainak célpontjai továbbra is a leggyakoribb eszközök és szoftverek sebezhetőségei. A vizsgált repülőterek közül csak 3 repülőtér „www." weboldala kapta meg a lehető legjobb „A+" besorolást, 15 repülőtér hivatalos weboldala pedig „A" besorolást nyert el. További 24 repülőtér weboldalát a legrosszabb, „F" kategóriába sorolták, ami azt jelenti, hogy elavult szoftverekkel rendelkeznek, amelyek ismert és kihasználható biztonsági réseket tartalmaznak az ügyfélkapcsolati rendszerben (CMS-ben[30] például WordPress) és a GDPR,[31]

[27] Saraogi (2019) i. m. 1.
[28] Azani–Lvovsky–Haberfeld (2016) i. m. 14.
[29] *State of Cybersecurity at Top 100 Global Airports.* Application Security Series, ImmuniWeb, 29 January 2020. 1.
[30] CMS: Content Management System – tartalomkezelő rendszer.
[31] GPDR: General Data Protection Regulation – általános adatvédelmi rendelet.

illetve a PCI DSS-előírásoknak[32] sem felelnek meg, esetleg a megfelelő SSL-titkosítás[33] is hiányzik.[34]

3.2. Mobilalkalmazás biztonsága

A kutatás 36 repülőtérhez tartozó hivatalos mobilalkalmazást is talált és tesztelt. Összesen 530 biztonsági és adatvédelmi kérdést azonosítottak, köztük 288 mobil biztonsági hibát (alkalmazásonként átlagosan 15). Ezenkívül a mobilalkalmazások külső szoftverkeretet tartalmaztak biztonsági résekkel, adatvédelmi és biztonsági problémákkal, valamint a titkosítás teljes hiányával.[35]

3.3. Sötét webes érintkezés és felhő

„Sötét" interneten a világháló azon részét értik, amelyet az eléréséhez szükséges technológiák és titkosítási eljárások miatt nem látnak a keresőszolgáltatások, és nem is elérhetők hagyományos böngészővel. Egy ilyen oldal megnyitásához speciális böngészőre van szükség, amely kezelni tudja a WebTOR nevű hálózatot, amelyben „.html" helyett „.onion" kiterjesztéssel találhatók meg a weboldalak. Ehhez általában a Tor Browsert szokták használni, amely kinézetre szinte teljesen megegyezik a Mozilla Firefoxszal, hiszen alapvetően ugyanarra a böngészőre épül, csak épp más keresőmotort használ.[36]

A kutatás szerint a vizsgált 100 repülőtér közül 66 valamilyen módon kapcsolódik a sötét webhez, kitéve magát az adatok kiszivárogtatásának és a kritikusinfrastruktúra-kockázatoknak. Emellett a repülőterek 3%-ánál nincs védett felhő az érzékeny adatok számára.[37]

A digitális infrastruktúrák rendkívül bonyolultak, ezért a digitális eszközök és a támadások felületének rendszerszintű láthatósága kulcsfontosságú a kiberbiztonsági program sikerének biztosítása szempontjából. Enélkül az erőfeszítések nem fogják a kívánt eredményeket meghozni.

4. Megoldások a repülőterek kiberellenálló képességének növelésére

A repülőterek kibertámadások elleni kitettségének és sérülékenységének minimalizálása, az úgynevezett kiberellenálló képesség javításával történik. Ez egy összetett és hosszabb átfutási időt igénybe vevő, az érintett szereplők közötti bizalomépítő hálózatos együttműködést, valamint az információk és az adaptálható legjobb gyakorlatok megosztását feltételező folyamat. Ennek főbb elemeit a következő alfejezetek részletezik.

[32] PCI DSS: Payment Card Industry Data Security Standard – bankkártyás fizetési adatvédelmi szabvány.
[33] SSL: Secure Sockets Layer – biztonságos információátviteli protokoll.
[34] *State of Cybersecurity at Top 100 Global Airports.* (2020) i. m. 1.
[35] Uo.
[36] *How to Access Dark Web: Dark Web, TOR Browser and Browsing. Onion Websites.* Forum Team, Blogstore, March 2020. 1.
[37] *State of Cybersecurity at Top 100 Global Airports.* (2020) i. m. 1.

4.1. Kiberellenálló képesség növelése a munkaerő és a szervezeti kultúra oldaláról[38]

- Munkaerő kiberbiztonsági képzettségi szintjének és kompetenciáinak szélesítése tudásátadó, tudásfelfrissítő továbbképzésekkel, tréningekkel, bevonásuk a döntéshozatali folyamatokba, felelősség és hatáskörök „testre szabott delegálásával". Szimulált kiberbiztonsági incidens gyakorlatok tartása (erre egy példa: az ENISA által Cyber Europe 2018 néven 30 ország bevonásával megszervezett, az egész európai légi közlekedést érintő, kibertámadás-sorozatot szimuláló kétnapos gyakorlata. Eszerint a reptéri automatikus bejelentkező terminálok váratlanul rendszerhibát jeleztek, majd az okostelefonok utazási applikációi álltak le, és a személyzet sem tudta használni számítógépeit a bejelentkező pultoknál. Mindezek következtében az utasok nem tudták feladni a csomagjaikat, valamint a biztonsági ellenőrzésen sem tudtak átjutni. Ilyen gyakorlatokra 2010 óta rendszeresen kétévente kerül sor).
- A kiberbiztonság legyen a szervezeti kultúra része, kiberbiztonsági stratégia kidolgozása a kiberbiztonsági incidensek megelőzése és hatékony kezelése érdekében.
- Hatékony külső és belső kommunikáció, információk megosztása, munkatársak közötti kapcsolatok javítása.
- Integritási kockázatok kezelése, titoktartás és hozzáférések feltételeinek megteremtése információbiztonsági szempontból.
- A repülőterek menedzsmentje és döntéshozói számára iránymutatások, amelyek ösztönzik és jutalmazzák a megfelelő kiberbiztonsági munkahelyi viselkedést, és támogatják az erre irányuló egyéni kezdeményezéseket.

4.2. Kiberellenálló képesség növelése a működési folyamatok, tőke- és kockázat-menedzsment[39] *oldaláról*[40]

- A kiberbiztonsági gyakorlatok kockázatalapú fejlesztésének ösztönzése a megfelelőség alapú megközelítés helyett, lehetővé téve a repülőterek számára, hogy feljebb lépjenek a „kiberbiztonsági érettség létrán".
- Különböző forgatókönyvek, protokollok kidolgozása a kiberbiztonsági incidensek kezelésére, megelőzésére, majd ezek kommunikálása, megismertetése a munkavállalókkal.
- Kiberbiztonsági kockázatok és hatásaik, felderíthetőségük beazonosítása.
- Új IKT-technológiák bevezetésének kiberbiztonsági kockázatai.
- A kiberbiztonsági kiadások betervezése a működési költségvetésbe.
- A kiberbiztonság mérésére mutatószámok kidolgozása, majd ezek alapján történő monitoringrendszer kiépítése és működtetése.

[38] *Advancing Cyber Resilience in Aviation: An Industry Analysis.* World Economic Forum, 2020. 16.
[39] *Securing Smart Airports.* (2016) i. m. 50–52.
[40] *State of Cybersecurity at Top 100 Global Airports.* (2020) i. m. 1.

- A beszállítói, alvállalkozói, üzleti partneri kapcsolatokban a kiberbiztonsági szempontok érvényesítése, külső ügyfelek jelentette információbiztonsági kockázatok felmérése.
- Hatékony kapcsolattartás az illetékes hatóságokkal, speciális információbiztonsági fórumokkal, szakmai szervezetekkel. Online fórumok, platformok létrehozása és működtetése, hogy a résztvevők egyeztessék álláspontjaikat a beérkező támadások és incidensek előzetes felmérése és értékelése kapcsán, továbbá kikérjék egymás véleményét, illetve a szabályok keretei között egyeztessék tervezett intézkedéseiket.

5. Következtetések

A repülőterek a technológiai innováció élvonalában vannak, mert az exponenciálisan növekvő légi és utasforgalom követelményeinek meg kell felelniük, valamint a Covid-19 koronavírus-járvány kihívásaira megfelelő válaszokat kell adniuk a talpon maradás érdekében. Ennek eredményeként a repülőtereknek javítani kell az infrastruktúra technikai intelligens eszközökön és megoldásokat kell kifejleszteniük, bevezetniük a stabil működésük érdekében, egyben kellemes utazási élményt nyújtva az ügyfeleknek, amely döntő szerepet játszik a repülési ágazat bevételeinek növelésében.

Az Ipar 4.0 és a digitalizáció során új kihívások jelentkeznek, amelyekhez a légi közlekedésnek gyorsan kell alkalmazkodnia. A kiberbiztonság a repülőterek szempontjából kiemelkedően fontos. Az intelligens repülőterek arra törekszenek, hogy megbízható és fenntartható módon biztosítsák az optimális szolgáltatásokat a növekedés, a hatékonyság és a biztonság egyidejű szem előtt tartásával.

A repülőtéri kiberbiztonsági kockázatok csökkentése több, egymással kölcsönhatásban levő megoldás[41] egyidejű megvalósításával lehetséges az alábbiak szerint:[42]

- Az adott repülőtér IBIR-rendszerének (információbiztonsági irányítási rendszer) kiépítése és működtetése az ISO 27001 szabvány előírásainak megfelelően. (A szabvány két részből áll: az informatikai biztonság menedzsmentjének gyakorlati kódexe, illetve ennek specifikációja). Ennek alapján célszerű a repülőtéri menedzsmentnek rendszeres kiberbiztonsági önértékeléseket végeznie: Milyen szintű és mennyire megbízható az információk védelme a széles körű fenyegetésektől? Mennyire adottak a feltételek a repülőtéri üzemeltetési folyamatok működésének folytonosságához, a legkisebbre csökkentve a kibertámadásokkal szembeni kockázatokat? Hol áll az adott repülőtér más repülőterekhez képest kiberbiztonság szempontjából?
- Az előzetes önértékeléssel feltárt helyzetkép alapján hosszú távú kiberbiztonsági stratégia kidolgozására kerülhet sor a kiberbiztonsági technikai és nem technikai incidensek megelőzése és kezelése érdekében, valamint fontos a vizsgálati eredmények alapján az azonosított sérülékenységek kijavítását célzó intézkedések megtétele is.
- Hatékony kiberbiztonsági monitorrendszer kiépítése és működtetése válik szükségessé az incidensek észlelésére, a kibertámadások blokkolására, az adathalászok és a jelszó-újrafelhasználási támadások kiszűrésére az ehhez szükséges erőforrások biztosításával.

[41] *Securing Smart Airports.* (2016) i. m. 50–52.
[42] *State of Cybersecurity at Top 100 Global Airports.* (2020) i. m. 1.

- A repülőterek informatikai rendszereinek és eszközeinek teljes körű naprakész nyilvántartása (vagyonleltár), valamint a külső támadási felületek és a kockázati kitettségek láthatóvá tétele olyan ASM-megoldással[43] lehetséges, amelyek a „sötét internet" és a kódtárak nyomon követesével is továbbfejleszthetők. A repülőtereket és a légi közlekedés működtetéséhez szükséges információkat osztályozni kell érzékenységük és kritikusságuk szerint a működést támogató szoftverek biztonsági szintjének beazonosításával, címkézésével és a biztonsági szabályzatnak megfelelő kezeléssel.
- Külső, független szakértők bevonásával egy kiberbiztonsági kockázatkezelési program dolgozható ki, amely magában foglalja a szállítók (beszállítók, alvállalkozók) folyamatos digitális nyomon követését, a kockázatok beazonosíthatóságát, hatásainak minimalizálását és a bekövetkezésük megelőzését.
- A munkavállalók kiberbiztonsági tudatosságát képzésekkel, tréningekkel (szimulációk, helyzetgyakorlatok, korábbi tapasztalatok, jó példák) lehet növelni, valamint információk megosztásán, egyéni kezdeményezések támogatásán, az információbiztonsági feladatok delegálásán keresztül alkalmasan képzett, tapasztalt és megfelelő hatáskörrel felruházott munkatársakkal, ahol minden munkakörben rögzíteni kell az adott munkatárs információbiztonsági felelősségét.

6. Összefoglalás

A negyedik ipari forradalom során minden gazdasági szektor, beleértve a légi közlekedési ipart is, digitális átalakulásban van: ennek hajtóereje a technológiai fejlesztések, a széles sávú internet (5G), mesterséges intelligencia, a felhőalapú számítástechnika, nagyméretű adatbázisok összekapcsolása (big data) és az adatok valós idejű feldolgozása, valamint az interneten egymással kapcsolatban lévő és egymással kommunikáló berendezések és eszközök (IoT). Ezek összetettsége és sérülékenysége megnöveli a különböző kibertámadási felületeket jelentős működési, pénzügyi és biztonsági kockázatokat hordozva magukban.

A kiberbiztonság napjaink egyik legnagyobb kihívása a repülési ágazat számára, ideértve a repülőtereket is. A repülőterek nagymértékben függenek a működő kritikus információs és kommunikációs rendszerektől üzemeltetési, személyszállítási és kommunikációs szempontból. Ezen technológiák megnövelték a repülőterek kitettségét a különféle kibertámadásokkal szemben. A világméretű, a polgári légiközlekedés elleni kibertámadások növekvő mértéke (körülbelül 200 különböző, a repülőterek földi és légi infrastruktúráit működtető, gyakran egymással is összefüggő rendszert érintenek ezek a támadások) és kifinomult technológiai megoldásai arra ösztönzik a repülőtereket, hogy tegyenek további lépéseket a kiberbiztonság javítására a repülőtéri műveletek és az utazóközönség védelme érdekében.

A kibertámadások elleni kitettség csökkentésére többféle módszer is létezik, de ahhoz, hogy a repülőterek és a légitársaságok meg tudják őrizni ügyfeleik bizalmát, új stratégiát kell kidolgozniuk. Ennek része kell hogy legyen egy olyan érzékelő és jelzőrendszer, amely a külső és belső rendszerek állapotáról folyamatos tájékoztatást ad kiberbiztonsági szempontból. Sikeres kiberbiztonsági stratégia és annak megvalósítása a szervezeti kultúrától függ. A kiberbiztonság,

[43] ASM: Attack Surface Managemenet – kibertámadásifelület-menedzsment.

az adatvédelem és a digitális bizalom mind azon alapul, hogy a szervezet sikerrel integrálja-e a biztonságot mint szervezeti elemet. Annak tudatosítása, hogy a kiberkockázat közös felelőssége minden érintettnek, a kibertámadások elleni megelőzéshez és védekezéshez szükséges megfelelő viselkedés kialakításával a kiberkockázatokkal szembeni ellenálló képesség csak növekedni fog a jövőben.

Felhasznált irodalom

A40-10: Addressing Cybersecurity in Civil Aviation. ICAO, 2019. Elérhető: www.icao.int/cybersecurity/Documents/A40-10.pdf (A letöltés dátuma: 2020. 06. 20.)

Advancing Cyber Resilience in Aviation: An Industry Analysis. World Economic Forum, 2020. Elérhető: www3.weforum.org/docs/WEF_Cyber_Resilience_in_Aviation_An_Industry_Analysis.pdf (A letöltés dátuma: 2020. 06. 15.)

Aviation Cyber Security – Moving Forwards. IATA, ICAO Working Paper on Assembly 40th Session Executive Committee, 2019. Elérhető: www.icao.int/Meetings/a40/Documents/WP/wp_395_en.pdf (A letöltés dátuma: 2020. 06. 15.)

Azani, Eitan – Lorena Atiyas Lvovsky – Danielle Haberfeld: *Trends in Aviation Terrorism.* International Institute for Counter-Terrorism (ICT), 2016. Elérhető: www.ict.org.il/UserFiles/ICT-trends-aviation-terror-aug-16.pdf (A letöltés dátuma: 2020. 07. 06.)

Effects of Novel Coronavirus (COVID-19) on Civil Aviation: Economic Impact Analysis. ICAO, 2020. Elérhető: www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf (A letöltés dátuma: 2020. 06. 16.)

Florent, R.: *Aerospace Cybersecurity: Building resilience in the hailstorm.* Cyber Inflight, 10 May 2020. Elérhető: www.cyberinflight.com/?p=1081 (A letöltés dátuma: 2020. 06. 16.)

How to Access Dark Web: Dark Web, TOR Browser and Browsing. Onion Websites. Forum Team, Blogstore, March 2020. Elérhető: www.blogstore.net/forum/web-site/how-to-access-dark-web-dark-web-tor-browser-and-browsing-onion-websites (A letöltés dátuma: 2020. 07. 06.)

Lam, Anthony – Jose Fernandez – Richard Frank: Cyberterrorists Bringing Down Airplanes: Will it Happen Soon? In A. R. Bryton – J. R. Lopez Jr. – R. F. Mills: *Academic Conferences and Publishing International Limited Reading.* Proceedings of 12th International Conference on Cyber Warfare and Security, Wright State University with the Air Force Institute of Technology Dayton, UK, 2–3 March 2017. 210–219.

Lykou, Georgia – Argiro Anagnostopoulou – Dimitris Gritzalis: Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors,* 19. (2019), 1. DOI: https://doi.org/10.3390/s19010019

Mazareanu, E.: *Coronavirus: impact on the aviation industry worldwide.* Statista, 4 Jun 2020. Elérhető: www.statista.com/topics/6178/coronavirus-impact-on-the-aviation-industry-worldwide/ (A letöltés dátuma: 2020. 06. 16.)

Pethuru, R. – A. C. Raman: *The Internet of Things. Enabling Technologies, Platforms & Use Cases.* CRC Press, Taylor&Francis Group, 2017. Elérhető: http://library.sadjad.ac.ir/opac//temp/19109.pdf (A letöltés dátuma: 2020. 07. 06.)

Saraogi, Varsha: *Five times airports were involved in cyberattacks and data breaches.* Airport Technology, 24 July 2019. Elérhető: www.airport-technology.com/features/

five-times-airports-were-involved-in-cyberattacks-and-data-breaches/ (A letöltés dátuma: 2020. 06. 17.)

Security and Facilitation Strategic Objective. Aviation Cybersecurity Strategy. ICAO, 2019. Elérhető: ww.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf (A letöltés dátuma: 2020. 06. 20.)

Securing Smart Airports. ENISA, Study, 2016. DOI: https://doi.org/10.2824/865081

State of Cybersecurity at Top 100 Global Airports. Application Security Series, ImmuniWeb, 29 January 2020. Elérhető: www.immuniweb.com/blog/state-of-cybersecurity-top-100-airports.html (A letöltés dátuma: 2020. 06. 21.)

Stouffer, Keith – Joe Falco – Karen Scarfone: *Guide to Industrial Control Systems (ICS) Security.* Recommendations of the National Institute of Standards and Technology, U.S. Department of Commerce, 2011. Elérhető: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf (A letöltés dátuma: 2020. 07. 06.)

Understanding Denial-of-Service Attacks. Cybersecurity and Infrastructure Security Agency, 20 November 2019. Elérhető: www.us-cert.gov/ncas/tips/ST04-015 (A letöltés dátuma: 2020. 07. 06.)