

A REPÜLÉS BIZTONSÁGI KÉRDÉSEI A XXI. SZÁZADBAN

„Bárki, aki más személyt szabadságától megfoszt, vagy hatalmába kerít és halállal vagy sérüléssel vagy további hatalomban tartással fenyeget abból a célból, hogy egy harmadik felet, nevezetesen valamely államot, nemzetközi kormányközi szervezetet, természetes, vagy jogi személyt, illetve személyek egy csoportját arra kényszerítsen, hogy az a tús elengedésének kifejezett vagy hallgatóságos feltételeként valamely cselekményt tegyen vagy ennek megtételétől tartózkodjon, az a jelen Egyezmény alkalmazásában a túszedés bűncselekményét követi el.”

(Túszedés Elleni Egyezmény, 1979. New York)

Bármilyen fejlett, korszerű technikával rendelkezik is egy állam, nem képes arra, hogy országa területének minden négyzetméterét ellenőrizze, megvédje valós vagy vélt támadásoktól. Erre azonban nincs is szükség. Vannak a biztonságúnak olyan kiemelt területei, amelyekre nagyobb figyelmet és több pénzt fordítva jelentősen lecsökkenthető a fenyegetettség lehetőség.

Napjainkban a polgári repülés — annak minden eleme, fázisa — az a terület, amely nagy figyelmet, és szigorúbb biztonsági intézkedéseket követel.

A biztonság elsősorban *adminisztratív és koordinációs fejlesztéseket* kíván, de a *technikai újítások és szigorítások* is elengedhetetlenek, hogy a nemzetközi polgári repülés jól védhető legyen a jogellenes beavatkozásokkal szemben. Az elmúlt évtizedek tapasztalatai alapján, de főleg a szeptember 11-i eseményeket követően, a repülőterek biztonsági rendszereinek fejlesztése egyre sürgetőbbé vált.

Az egyik legfontosabb terület, amely fejlesztést kíván, az *átvilágító berendezések* korszerűsítése. A legtöbb átvilágító rendszer 20–30 éves technológián alapul, amely csak az acél, illetve egyes ötvözetek kimutatására alkalmas.

A legújabb technológia a repülőtéri biztonsági rendszerek között a számítógéppel támogatott előzetes utasátvilágító rendszer, a CAPPS (Computer Assisted Passenger Prescreening System). Ilyen rendszer telepítése zajlik most a Ferihegy Repülőtér 2A terminálján. A tervek szerint egy többszintű vizsgálóberendezés kerül majd alkalmazásra a telepítés után a terminálon. Ennek az a lényege, hogy az átvilágítás során a csomagokat több berendezés is vizsgálja. Az első röntgenberendezés azokat a csomagokat, amelyeket nem talál gyanúsak, továbbengedi. Annak a csomagnak a röntgen-képét, amelyekben talál valami veszélyesnek tűnő tárgyat, a berendezés kezelőjéhez továbbítja, aki, ha úgy gondolja, valóban van valami gyanús a csomagban, a harmadik gép felé küldi a csomagot. A harmadik gép már csak a megjelölt területet vizsgálja meg alaposabban, végül a gyanús csomag a biztonsági személyzethez kerül majd, akik jogosultak a csomag felnyitására, átvizsgálására, természetesen csak a csomag tulajdonosának jelenlétében.

A polgári repülés támogatásában még mindenképpen új rendszernek számít a gyógyászatban már alkalmazott CT — computer tomográfias berendezés. Az utasok és a csomagok átvilágításához olyan Röntgen-sugaras berendezést fejlesztettek ki, amely a computer tomográfias technoló

gián alapul. Bár ennek telepítése és üzemben tartása rendkívül költséges, a rejtett, idegen tárgyak felfedezésének egyik talán legbiztosabb módja napjainkban a polgári légiközlekedési biztonság terén.

Ma már egyre több helyen alkalmazzák az átvilágító személyzet kiképzése folyamán az ún. Threat Image System-et (TIP), amely elektronikusan generálja a különböző lehetséges támadóeszközök (pisztoly, kés, robbanóanyag) átvilágított képét, és megjeleníti azokat a Röntgensugaras, vagy robbanóanyag-detektor rendszerek kijelzőin, úgy, mintha azok egy átvilágított csomagban lennének. A rendszer és a kiképzés célja, hogy tapasztaltabbá és éberebbé tegye az átvilágító személyzetet, akik nem minden nap találkoznak ilyen támadóeszközökkel, s monoton munkájukból adódóan figyelmük érthetően egyre kisebb lesz az órák múltával. Stumphauer Imre rendőr alezredes szerint — aki a ORFK Repülőtéri Biztonsági Szolgálat kiképzési csoportvezetője — ez a kiképzési módszer igen hatékony, Ferihegyen is alkalmazzák az átvilágító személyzet kiképzésénél. A rendszer megbízható és hiteles képeket generál a csomag veszélyes elemeiről, amelyeket a kezelőnek pár másodperc alatt kell felismernie.

A nagyobb biztonság érdekében a US National Institute of Standards munkatársai egy olyan rendszer prototípusán dolgoznak, amely a csomagok és utasok átvilágítása során képes megtalálni a rejtett fegyvereket, plasztik támadóeszközöket. Ez napjainkban egyre fontosabbá válik, hiszen a terroristák nap mint nap új támadóeszközökkel állnak elő, s ezek nagy része ma már olyan anyagokból áll, amelyeket szinte csak elemeiből lehet kimutatni. Így például a Sandia National Laboratories munkatársai olyan berendezésen dolgoznak, amely hatóanyagai alapján közel 90%-os biztonsággal képes kimutatni a kémiai vagy robbanóelegyek jelenlétét.

A ma már létező, de a — kevés kivétellel — repülőtereken még nem alkalmazott biometria azonosító rendszerek a jövőben kulcsfontosságú részét képezik a biztonsági fejlesztéseknek.

Ezek a berendezések az utasokat, a repülőtéri és légi személyzetet egyedi biometria adataik alapján azonosítják, mint például az ujjlenyomat, az arc vagy a kéz geometriai jellemzői, a retina sajátos vonásai, vagy a hangszín.

Ezeket az információkat egy virtuálisan feltörhetetlen, kódolt szoftverrel ellátott, ún. „*ügyes kártyán*” (SC — smart card) tárolják, amely az egyik része az azonosítási eljárásnak. Az SC-ok előnye, hogy ha valaki el is veszíti a kártyáját, azt más nem használhatja fel, hiszen adatai nem egyeznek a chipben tárolt biometria jellemzőkkel. A Chicago O'Hare repülőtéren már alkalmazzák az ujjlenyomat-azonosító berendezéseket a biztonsági személyzet és a csomagellenőrző-és elosztó személyzet ki-és beléptetésére. Ez a módszer a tapasztalatok szerint 2–4-szer hatékonyabb, gyorsabb és biztonságosabb, mint a hagyományos, manuális rendszer. A Charlotte/Douglas repülőtéren pedig az írisz-azonosító technológiát alkalmazzák sikeresen az alkalmazottak azonosítására egyes biztonsági területre. Az SC-k elterjedése komoly technológiai háttérrel igényel, de a gyors ütemű fejlődést tekintve csupán néhány év kérdése lehet, hogy a Föld népességének jelentős hányada — a légiközlekedésben érintetteknek pedig közel 80%-a — rendelkezzen biometria azonosítót tartalmazó, személyazonosságot igazoló kártyákkal.

A repülőgép-eltérítés kritikus pontja, hogy a gépeltérítő *hogyan jut be a pilótafülkébe*, és hogy a személyzet, illetve az utasok mennyire együttműködők a jogellenes beavatkozás során.

A repülőgép-gyártók a biztonság növelése érdekében új eljárásokkal próbálják növelni a *pilótafülke biztonságát*. A Virgin Atlantic például a pilótafülke ajtaját *golyóálló ötvözetből* készí

tette el, ezen kívül minden ajtón belülről alumínium és acél tolózárr van, amely golyó-, hő- és ütésálló, 800 tonna nyomást bír ki, és digitálisan vezérelt a nyitása, illetve zárása.

Hatékony lehet a légijármű személyzetének — pilóták, légikisérők — önvédelmi- és válságkezelési kiképzése is, amely magába foglalja a fizikai, pszichikai felkészítést, a támadó megnyugtatót, lefegyverzését, az utasok közvetlen védelmét.

Emellett az FAA javaslatot dolgozott ki az ún. *Légi Békebíró Programra* (Air Marshal Program). A program lényege, hogy magasan képzett, katonai vagy egyéb fegyveres szervnél szerzett tapasztalatokkal rendelkező légi békebírókat alkalmaznak a repülőgépek fedélzetén. A békebírók rendelkezhetnek fegyverrel, amely az előzetes tervek szerint valamilyen kábítófegyver, esetleg elektrosokk, hogy amennyiben annak alkalmazására kerülne sor, az ne veszélyeztesse a repülőgép és az utasok épségét. A járatók nagy reményeket fűznek a programhoz, több nemzetközi légitársaság már kísérleti céllal alkalmaz „légi biztonsági őröket”.

Nagy gondot és kihívást jelent a *légiforgalmi irányító rendszerek*, számítógépes hálózatok védelmének fejlesztése, ugyanis ezek a rendszerek nélkülözhetetlen adatokat, információkat szolgáltatnak mind a légiforgalmi irányítóknak, mind a pilótáknak a légijármű biztonságos üzemelése érdekében, amelyeknek megzavarása katasztrofális következményekkel járhat. Nagyon fontos, hogy ezek a rendszerek a megfelelő teljesítményű hardver, szoftver és kommunikációs eszközökkel dolgozzanak.

Az *analóg* légiforgalmi irányítói berendezéseket napjainkra szinte teljesen kiszorítja a *digitális* technológián alapuló, műholdas navigációt alkalmazó telekommunikációs és irányító rendszer. Ezek az újítások nagymértékben megváltoztatják a repülések gyors és hatékony kezelésének eddigi módszereit.

A földi telepítésű légiforgalmi *irányítás* (analóg rádiók, navigációs körsugárzók és radarok) helyett egy sokkal hatékonyabban működő légiforgalmi *szervezés/management* (digitális kommunikáción és műholdas navigáción alapul, ahol a pilóták és a légiforgalmi irányítók döntéseit nagyteljesítményű számítógépes rendszerek támogatják) kerül kiépítésre.

Az információs rendszerekkel szemben, amelyek egyben művelettámogató rendszerek is, alapvető követelmény, hogy *automatizáltak* legyenek, hiszen óriási mennyiségű adathalmazt dolgoznak fel: radaradatok, időjárási információk, előrejelzések, repülési terv nyilvántartása és feldolgozása, légtérellenőrzési információk, navigációs és leszállító berendezések adatai, forgalomszervezés és koordinálás, kommunikációs összeköttetés a légijármű és az irányító személyzet, illetve a különböző irányítói munkahelyek között.

Biztosítani kell a szolgáltatás folyamatosságát, illetve a rendszereket el kell látni ún. behatolás felderítő és riasztó programmal, ugyanis a nagymértékű számítógépesítés, automatizálás nemcsak hatékonyabbá, de sebezhetőbbé is teszi a rendszert, s a nem megfelelő védelem növelheti a légi balesetek és a *cybertámadások* eshetőségét, mivel a nélkülözhetetlen adatokat közvetítő hálózat folyamatosan ki van téve a hackereknek, cyberterroristáknak, akik az adatok manipulálásával veszélyeztetik több száz ember életét.

Mi jelenthet megoldást a folyamatosan támadó cyberterroristák ellen? A repülés szempontjából fontos navigációs és meteorológiai műholdak olyan valós idejű adatokat közvetítenek, amelyek nélkülözhetetlenek a légijármű személyzete és a légiforgalmi irányítók számára.

Az ún. CNS rendszer — kommunikáció, navigáció, légtérellenőrző-felderítő rendszer — már magába foglalja a műholdas navigációt, amely napjainkban még olyan technológiát képvisel, amelyet nem lehet házilag készített eszközökkel, személyi számítógépekkel zavarni, befolyásolni. Úgy tűnik tehát, hogy a műholdas technikán alapuló légiforgalom szervezés és ellenőrzés jelentheti a megoldást a repülésirányító rendszerek biztonságára.

A műholdak esetében a biztonság többszörösen összetett kérdés. A műholdak azonosítására egyrészt az ezred-másodpercenként ismétlődő C/A kód szolgál, amely nem más, mint egy bináris számsorozat, amelyben két szám váltakozásával történik meg az egyedi azonosítás.

A másik azonosítási mód az ún. P kód, amely 266,4 nap ismétlődési idejű, amelyet hét napos időszakokra bontottak szét. A kódot minden vasárnap éjfélkor állítják be, és az azonosító PRN szám azt mutatja meg, hogy a teljes periódusú P kód melyik 7 napos szakaszát rendelték hozzá az adott mesterséges műholdhoz.

Az illetéktelen beavatkozás megakadályozása érdekében alkalmazzák az Anti-Spoofing (A-S) eljárást, amellyel titkosítják a P kódot, így jön létre az Y kód. A nagyobb biztonság érdekében a holdak által kisugárzott navigációs információkat is kódolják, amelyet 50 Hz frekvenciájú jelekkel oldanak meg.

A műholdas rendszer alkalmazásakor fontos kérdés a rendszer védettségének szintje. A BLOCK II.R. típusú műholdak például védettek neutron-és lézerfegyverek ellen, földi eszközökkel pedig, a nagy pályamagasság miatt, amely több mint 20 000 km, nem semmisíthetők meg.

Ezek a rendszerek többszörös kóddal védett hálózatok, az általuk közvetített, kódolt adatokhoz illetéktelenek nem férhetnek, hiszen az adatátvitel olyan csatornákon történik, amelyet személyi számítógépekkel, elektronikai zavaró eszközökkel nem lehet megzavarni.

A műholdas rendszerek kiépítése és karbantartása kétségtelenül költségesebb, mint egy kiterjedt számítógépes és kommunikációs hálózat létrehozása, de biztonságát tekintve ezek a plusz költségek rövid időn belül megtérülhetnek.

A repülés biztonságának egyik fontos eleme az *azonosítás*. Bármely modern légiforgalmi irányító rendszerben a repülőgépek azonosításának egyik alapvető módszere a másodlagos felderítő lokátorok (Secondary Surveillance Radar — SSR) használata.

A Mode S kivételével a jelenlegi SSR rendszer képes a levegő-föld vonalon információt biztosítani az 1030–1090 MHz sávon. A katonai repülőgépek a légiforgalmi irányításban használt módja vagy csatornája (Mode 3) kompatibilis a polgári megfelelőjével (Mode A). Általában jelölésük a Mode 3/A.

Az SSR működés alapja az, hogy a repülőgép fedélzeti válaszadójára a földi állomás rákérdez, ami egy kódolt választ vált ki. A földi állomás így azonosítja a repülőgépet. Az SSR működés alapja az, hogy a repülőgép fedélzeti válaszadójára a földi állomás rákérdez, ami egy kódolt választ vált ki. A földi állomás így azonosítja a repülőgépet.

Bár a terrorizmus főbb célpontjai a polgári repülőgépek, illetve utasok, nem zárható ki annak lehetősége sem, hogy egyes terroristák *katonai légijárművek* feletti ellenőrzés megszerzésével próbálnak meg érvényt szerezni követeléseiknek.

1994. júliusában egy hivatalos NATO állásfoglalást adtak ki a Mode S-ről. Ez a dokumentum elismeri a Mode S transzponderek katonai repülőgépekbe történő beszerelésének és üze

meltetésének szükségletességét, annak érdekében, hogy megkönnyítsék ezen repülőgépek hozzáférését a polgári irányítású légterekhez (pl.: polgári ATS — útrendszer).

Az azonosítás azért nagyon fontos, mert a Nemzeti Légtérellenőrző Csoport a fedélzeten beállított azonosító kód alapján biztosítja, hogy a légtérben működő légijárművek ismert forgalmak, s ellenséges szándékuk nincs. Az azonosító kóddal nem rendelkező, vagy hibás azonosítót jelző légijárműveket ún. elfogó vadászrepülőgépek segítségével azonosítják. *De mi történik akkor, hogyha válság vagy háborús helyzetben, esetleg egy légi harc esetén illetéktelenek megzavarják az azonosítási rendszert, s légvédelmi rendszereink saját gépeinket ellenségként azonosítják és kezelik?*

A katonai harcászati vagy szállító repülőgépeknek korlátlan hozzáféréssel kell rendelkezniük a légtérhez kiképzési, hadműveleti alkalmazás vagy a kiképző és hadműveleti légterekbe történő kitelepülés érdekében. Azon területeken, ahol a katonai kiképzési hadműveleti légterek a Mode S környezetben találhatók, ott az eljárásoknak és eszközöknek képesnek kell lenniük a lényeges információk eljuttatására, mind a polgári mind a katonai repülőszemélyzetekhez és irányítókhoz, úgy, hogy az ne veszélyeztesse a repülésbiztonságot, a hatékony légiforgalmat vagy a térségben folyó katonai kiképzést vagy hadműveleti tevékenységet.

Tekintettel arra, hogy a Mode S-t nem úgy tervezték, hogy rádióelektronikai harc körülményei között is képes legyen ellátni feladatát, ezért szükség esetén egy különálló, független katonai *IFF* (Identification Friend or Foe — Idegen-barát azonosító rendszer) rendszert vagy módot kell a katonai hatóságoknak használnia, hogy az a hadműveleti követelményeknek biztonsági és zavarvédelmi szempontból megfeleljen.

Kérdés, hogy a pontos frekvencia ismeretében mennyi időt vesz igénybe az, hogy akár a földről, akár egy levegőben lévő légijárműről, amely megfelelő zavaró berendezésekkel van felszerelve, megzavarják a légijármű azonosításának menetét, ezzel veszélyeztetve a légiforgalom biztonságos áramlását, legyen az polgári vagy katonai forgalom.

Összességében tehát elmondható, hogy a légiközlekedés mint napjaink nélkülözhetetlen eleme olyan, egyre növekvő veszélyeknek van kitéve, amelyeket komolyan kell venni, ellenük gyorsan és hatékonyan kell fellépni. A fejlesztések, a szigorítások elengedhetetlenek ahhoz, hogy a jövőben elejét vegyük olyan támadásoknak, amelyek a polgári vagy a katonai repülés elemeit használják fel terrorista célok érdekében.

FELHASZNÁLT IRODALOM

- [1] Civil-katonai együttműködés a légiforgalom kezelésének területén AC/92-WP/407, NATO nyílt.
- [2] Air traffic control weak computer security practices jeopardize flight safety, U.S. General Accounting Office GAO/AIMD-98-155, 1998. Mai.
- [3] Robert D. Atkinson: Aviation security systems for 21st century must fully incorporate latest technologies, ICAO Journal No. 5.
- [4] Sam Nunn: Get Ready for Cyberwar, Blueprint Magazine, 2000. January.
- [5] Stephen Barlay: The Final Call – Air Disasters...When will they ever learn? Sinclair-Stevenson Ltd., London, 1990.
- [6] AGARD-R-825 Air Traffic Management: Support for Decision Making Optimisation – Automation, 1997.
- [7] Todd O’Boyle: Cyberspace Detectives Employ Intrusion Detection Systems and Forensics, The EDGE Newsletter, 2001. February.
- [8] Deployment of Federal Screeners, U.S. Department of Transportation, Sept. 4. 2002.
- [9] Combating Terrorism U.S. General Accounting Office T-NSIAD-98-164.