HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 2. szám 97–106.
DOI: 10.32567/hm.2024.2.8

Fazekas Gábor[1]

Oldalsávi információszivárgás mint valós fenyegetettség

Side-Channel Attack is a Real Threat

Absztrakt

Korunk védelmi iparának egyik kulcsfeladatköre az információbiztonság, amelynek emberi és technikai függései rendkívül sokrétűek. A vállalati és kormányzati szervek informatikai rendszerei folyamatos felügyeletet, fejlesztést és auditot igényelnek, amelyek kiterjednek az emberi munkaerőre is. Ennek egyik oka, hogy a mobil és egyéb szórakoztató elektronikai eszközök iránt a piaci kereslet már évekkel a koronavírus megjelenése előtt hatással volt az ipari ellátási láncokra, kezdve az elektronikai alkatrészek gyártásától a telekommunikációs protokollokon és a mesterséges intelligencián keresztül a fejlesztési módszertanokig. Ez az ipar folyamatos átalakulásához vezetett, ami maga után vonta az elektronikai eszközök fejlesztési idejének lerövidülését is. Végeredményképp olyan minőségű hardver-, szoftver- és módszertani eszközök váltak széles körben elérhetővé a civil lakosság számára, amelyek valós sebezhetőséggé emeltek egy addig mítoszként kezelt jelenséget. Kutatásomban a kisugárzásvédelem egy szegmensét, a passzív elektromágneses információszivárgást, illetve fenyegetettsége növekvő hatását és okait mutatom be. Kutatásom célja egy innovációs tevékenység során előállított saját fejlesztésű eszköz megvalósításán keresztül szemléltetni, hogy a civil lakosság által is hozzáférhető és megfizethető COTS (commercial off the shelf – kereskedelmi forgalomban elérhető) eszközök, szoftverek és a korszerű modellalapú fejlesztési gyakorlat segítségével mára valós fenyegetettséggé vált az elmúlt évtizedek során kizárólag az állami szereplők által alkalmazott megfigyelési technika.

Kulcsszavak: EMSEC, információbiztonság, MBD, SDR, TEMPEST

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: fazekg@gmail.com

Abstract

One of the key tasks of the defence industry of our time is information security, of which human and machine dependencies are extremely diverse. The IT systems of companies or government agencies require continuous supervision, development and audits, which also extend to the human resource. One of the reasons for this is that the market demand for mobile and other entertainment electronic devices subvert the industrial balance of power years before the emergence of the coronavirus, starting from the production of electronic components, through telecommunication protocols and artificial intelligence to development methodologies. This led to a continuous transformation of the industry, which entailed the shortening of the development time of electronic devices. As a result, high-quality hardware, software and methodological tools became widely available to the civilian population, which raised a phenomenon that had been treated as a myth to a real vulnerability. In my work, I present a segment of emission security, the leakage of passive electromagnetic information, and the growing trend and causes of the threat. The purpose of this publication is to illustrate through my own R&D, that with the help of COTS (Commercial Off the Shelf) devices, software and modern model-based development practices that are accessible and affordable to the civilian population, the observation techniques used exclusively by professional services in the 1950s, has now become a real threat.

Keywords: EMSEC, information security, MBD, SDR, TEMPEST

Bevezetés

Korunk társadalmában az információvédelem kiemelt fontosságú terület. Az információszivárgás témakörében a legritkább esetben említik az oldalsávi támadásokat *(side channel attack)*, vagyis a TEMPEST-et, amely napjainkra a civil szférát is érintő fenyegetettséggé vált. Az oldalsávi támadások olyan módszerek, amelyek fókuszában nem közvetlenül az információs csatorna áll, hanem az egyes informatikai rendszerek működéséből adódó egyéb fizikai jelenségek, például elektromágneses sugárzás, mechanikai rezgések vagy hőmérséklet-változás. Ezen jelenségek specifikus szenzorokkal detektálhatók és rögzíthetők, digitális jelfeldolgozási eljárásokkal pedig ezen csatornákon érzékeny adatokat nyerhetünk ki a célrendszerekből.

A vezeték nélküli telekommunikációs eszközök iránti piaci igény az ipart a nagy integráltságú, jó minőségű és tömeggyártott rádiófrekvenciás eszközök kutatása és fejlesztése felé terelte. Ennek, illetve a hatékony fejlesztést elősegítő MBD (*model based design* – modellalapú fejlesztés) módszertannak köszönhetően a polgári területeken is lehetséges az elektronikai eszközök elektromágneses felderítése és megfigyelése.

Kutatásom céljául tűztem ki, hogy polgári felhasználású komponensekből előállítsak egy olyan kísérleti eszközt, amely képes lehet LCD-monitorok oldalsávi elektromágneses sugárzásából származó információ, vagyis a megjelenített kép rekonstrukciójára. Ezzel rá szeretnék világítani a polgári lakosság esetleges fenyegetettségére, illetve a hazai TEMPEST-megfelelőségi kritériumok kidolgozásának fontosságára.

Az oldalsávi információszivárgás

Egy 1972-ben az amerikai Nemzetbiztonsági Szolgálat (NSA – National Security Agency) által írt, 2007-ben a titkosítás alól részben feloldott jelentés több, a témát érintő eseményről számol be. Az egyik ilyen eset a második világháború alatt történt a 131-b2 távíró rejtjelező géppel kapcsolatban, amelyet a Bell Laboratórium fejlesztett ki az Amerikai Egyesült Államok hadserege híradó csapatainak (USASC – United States Army Signal Corps) részére. Az eszköz már rendszeresítve volt a hadseregben, amikor egy Bell-mérnök észlelte, hogy a rejtjelező gép üzemszerű működésének indulásakor a laboratórium egy távoli részén található oszcilloszkóp kijelzőjén zavarok jelennek meg. A jelenséget vizsgálva kiderült, hogy a kilengések mértéke a rejtjelezendő üzenettől függően változik, tehát azok bizonyos mértékig visszafejthetők. Mivel az esetet a Bell biztonsági hiányosságként értékelte, tájékoztatták róla a híradó szervezeteket. A választ szintén tartalmazza a jelentés: „Nem veszed észre, hogy háború van? Egy kétes és ezoterikus laboratóriumi jelenségre alapozva nem állíthatjuk meg kriptográfiai műveleteinket. Ha ez valóban veszélyes, bizonyítsd be." Ennek megfelelően a Bell munkatársai elutaztak New Yorkba és a USASC rejtjelközpontjával szemben (Varick st.), attól 80 láb (24,4 m) távolságra települtek ki. Egy óra mérés alatt az üzenetek 75%-át sikerült visszafejteniük. Az esetet követően a hadsereg lefektetett néhány információvédelmi alapelvet a védelmi távolság, elektronikus árnyékolás és a zavarás tekintetében.[2]

Bár a háború rövidesen véget ért, a projekt bizonyosan tovább élt a hidegháborús környezetben. Az elektronikus adatfeldolgozó rendszerek kompromittáló kisugárzásának analízise tehát nagyságrendileg a második világháború óta képezi az információvédelem részét. Az 1980-as évek közepéig mértékadó publikus információ nem látott napvilágot e témában. Ezen változtatott Wim Van Eck holland számítógépmérnök 1985-ben megjelent cikke, amelyben a szerző egy CRT (*cathode ray tube* – katódsugárcső) monitor oldalsávi elektromágneses kisugárzását kihasználva rekonstruálta a monitoron megjelenő képet.[3] Markus Kuhn és társai több cikkben vizsgálták különböző eszközök elektromágneses kisugárzását mint biztonsági sebezhetőséget, majd 1998-tól Kuhn több cikket is publikált a monitorok lehallgathatóságáról.[4] Az eddigiek alapján kijelenthetjük, hogy az elektronikus eszközök hordoznak egyfajta lehallgathatósági rizikófaktort,[5] amelyet a besorolási szinthez mérten kell kezelni. Több terminológia is született a terület és a kapcsolódó eszközök vonatkozásában, úgymint: EMSEC (*emission security* – kisugárzásbiztonság), TEMPEST, illetve oldalsávi információszivárgás. Fontos megjegyezni, hogy jelen munka kizárólag az elektromágneses kisugárzással kapcsolatos, bár a jelenség nem csupán a nem szándékosan előállított elektromágneses hullámok detektálását érinti, hanem a hang-, optikai és egyéb kommunikációs tartományokat is.

[2] NSA 1972: 27.
[3] Eck 1985.
[4] Kuhn–Anderson 1998; Kuhn 2005.
[5] Kuhn 2003.

A TEMPEST magyarországi szabályozása

Magyarország TEMPEST-hatósága a Nemzeti Biztonsági Felügyelet (NBF), amely honlapján a következő definíciót használja:

„Minden elektromos eszköz bocsát ki magából elektromágneses jeleket. Ez a fizikai jelenség lehetővé teszi, hogy megfelelő eszközök alkalmazásával a kisugárzott jelekből reprodukálható legyen az eszközön kezelt eredeti adat. Minősített adat elektronikus úton történő kezelése esetén a kompromittálódás elleni fő feladat a minősített adatot tartalmazó kisugárzás minimális szintre történő csökkentése, ami megakadályozza az adat reprodukálhatóságát, annak illetéktelen kezekbe jutását. E módszer és a rá vonatkozó szabályok összefoglaló neve a TEMPEST."[6]

Magyarországon erre vonatkozó nyílt utalás mindössze a 41/2015. (VII. 15.) BM rendelet 3. mellékletének 3.3.10.14.4 Antennák alfejezetében található: „Az érintett szervezet olyan karakterisztikájú és teljesítményszintű antennákat és árnyékolási megoldásokat üzemeltet, vagy egyéb technikákat alkalmaz, amelyekkel csökkenti az érintett szervezet fizikai védelmi határain kívül a jelek észlelésének a valószínűségét."[7]

Az ezredfordulót követően a kisugárzásvédelmi témakörben folyamatosan növekvő kutatás-fejlesztési aktivitást óvatos kormányzati alkalmazkodás kíséri.[8] Erre a jelenségre a lehetséges magyarázatot a technológiai és a kutatás-fejlesztési tevékenységek módszertani fejlődésében kell keresnünk.

A fejlesztőkörnyezet

Az ezredfordulóig a széles sávú rádióvételnek jelentős költségvonzata volt. A mobilkommunikáció globális elterjedése és folyamatos fejlődése az egyre növekvő integráltságú rádiómodulok fejlesztését, gyártását vonta maga után. Az SDR-ek (*software defined radio* – szoftverrádió) (1. ábra) megjelenésével átalakultak a fejlesztői diszciplínák: a szoftveres alapsávi moduláció lehetősége közel hozta egymáshoz az informatikát és a rádiótechnikát.

Egy SDR kimenetéről érkező több MSps (*mega sample per second* – millió minta per másodperc) sebességű jelfolyam feldolgozása egy hagyományos PC-t (*personal computer* – személyi számítógép) használva valós időben nem megoldható. Bár az FPGA-k (*field programmable gate array* – programozható logikai hálózat) órajel-frekvenciájukat illetően elmaradnak a személyi számítógépekétől, azonban felhasználásukkal valódi párhuzamos művelet-végrehajtást érhetünk el, ezzel lehetővé téve a valós idejű jelfeldolgozást. A véges impulzusválaszú vagy FIR- *(finite impulse response)* szűrők neurális hálózatokon vagy egyéb nemlineáris dinamikus rendszereken alapuló adaptív szűrők. Ezek összességében egyszerű logikai alapelemekből felépíthető rendszerek,

[6] NBF.

[7] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

[8] Kuris 2010: 182–183.

amelyek esetében az FPGA egy ideális feldolgozóegység, mivel segítségével valós időben több, egyszerű művelet egyidejűleg hajtható végre. Ez a képesség szoftverrádiók alapsávi IQ- (a komplex jel csatornái: képzetes és valós) jeleinek kezelése során elengedhetetlen, ezért a valós idejű, széles sávú modulációs/demodulációs sémák alkalmazására és szűrésére jelenleg az FPGA optimális megoldást kínál.

1. ábra: LimeSDR szoftverrádió
Forrás: a szerző felvétele

Kutatásom során az egyszerű beszerezhetőség és az elérhető ár miatt az RTL-SDR szoftverrádiót használtam. Ezen eszközt eredeti rendeltetése szerint földfelszíni televízióműsor vételére fejlesztették, azonban alacsony ára miatt széles körben elterjedt a rádióamatőrök közrében is. Lényeges tulajdonságai:

- az alapsávi IQ-jelet USB-n keresztül továbbítja a számítógépnek;
- vételi frekvenciatartománya 100 kHz-től 1,7 GHz-ig terjed;
- maximális sávszélessége verziótól függően 1–3 MHz között van.

Népszerűsége miatt az eszközt számtalan rádiószoftver támogatja, mint például a GQRX, az SDRCube és a DAB Player. Ezen programok jellemzően kereskedelmi rádió- és televízióadások demodulációjára alkalmasak, ugyanakkor elérhetők olyan fejlesztői lehetőséget biztosító programok is, amelyek alkalmasak akár saját modulációs/demodulációs technológiák létrehozására, implementálására. Ilyenek például a GNURadio vagy a MATLAB.

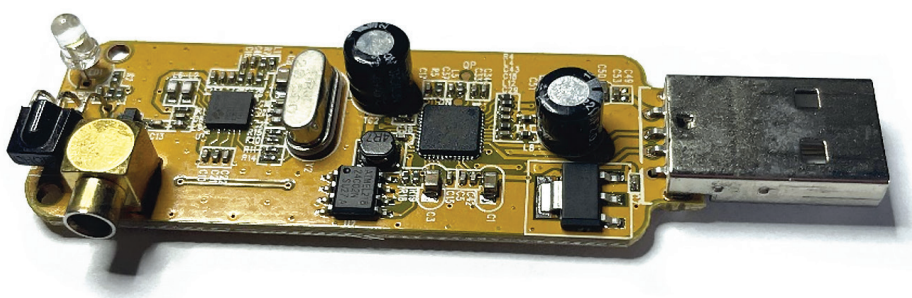
Felderíthetőség megállapítása

Jelenleg a NATO SDIP-27/2 szabványa rendelkezik az elektronikai eszközök kisugárzással szembeni védettségi szintjének megállapításáról az alábbiak szerint:[9]

- NATO SDIP-27 Level A – USA NSTISSAM Level I,
- NATO SDIP-27 Level B – USA NSTISSAM Level II,
- NATO SDIP-27 Level C – USA NSTISSAM Level III.

Az információszivárgással kapcsolatos határértékek, illetve mérési körülmények minősítettek, így számomra csupán relatív mérések elvégzésére nyílt lehetőség, amelyhez az eredeti kép közeltéri visszaállíthatóságának mértékével arányos saját kritériumokat állítottam fel. Bár a visszaállított kép felbontása arányos a vételi oldal sávszélességével, így a rádió sávszélességének növelésével a lehallgatott kép minősége is javul,[10] a visszaállított kép kontrasztossága kis sávszélességgel is biztosítható.

Jelen vizsgálat tárgya, hogy valóban jelenthet-e veszélyforrást a néhány ezer forintért beszerezhető RTL szoftverrádió (2. ábra).

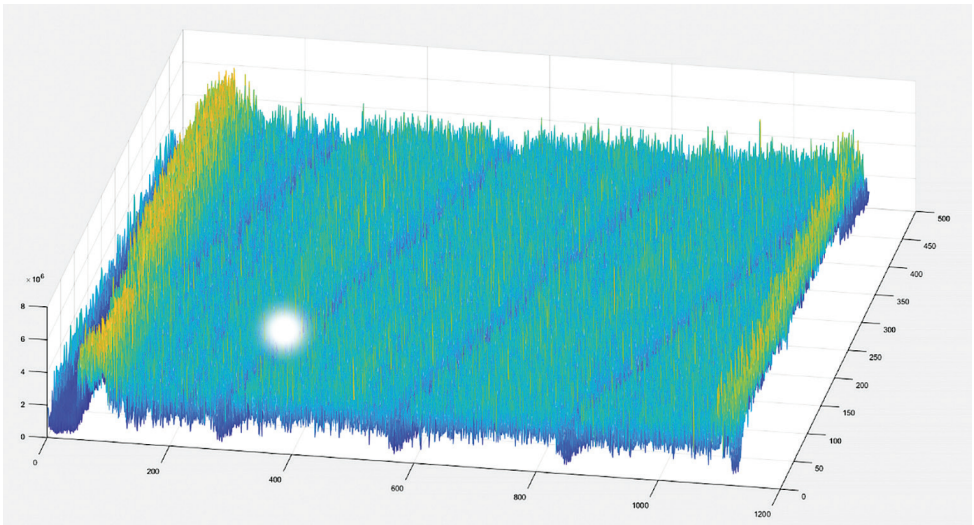


2. ábra: Pendrive méretű RTL-SDR szoftverrádió
Forrás: a szerző felvétele

Bár az eszköz sávszélessége kicsi, a modellalapú fejlesztési technikák alkalmazásával és saját demodulációs technika kifejlesztésével sikeresen detektáltam egy LCD-monitor szinkronjeleit (3. ábra).

A szoftverrádió mágnestalpas vevőantennáját ebben az esetben a vizsgált monitor közvetlen közelében helyeztem el, és a jelfeldolgozás offline volt, vagyis azt a szoftverrádió nyers alapsávi IQ-jeleinek rögzítése után, nem valós időben, MATLAB-bal végeztem. A mérés során több vivőfrekvencián mintavételeztem, majd ezeket az általam implementált raszterezésre is képes demodulátor-algoritmussal jelenítettem meg. Miután egyes frekvenciákon láthatóvá váltak a szinkronjelek, néhány MHz eltolással újabb jelrögzítést hajtottam végre. Ez hatásos stratégiának bizonyult a kompromittáló jelek felderítésében.

[9] Shopina 2020.
[10] Marinov 2014.



3. ábra: Monitor kisugárzásából visszaállított PAL szinkronjelek
Forrás: a szerző szerkesztése

A felderítés és képvisszaállítás hatékonyságának fokozásához a rendszer valós idejű jelfeldolgozási képességének kialakítása vált szükségessé. Mivel az RTL-SDR kis sávszélességű, egy személyi számítógép is elegendő a valós idejű jelek feldolgozására. A valós idejű mintavételezés és feldolgozás során a demoduláció módosításával, rádióspecifikus finomhangolással, illetve valós idejű feldolgozással elértem az eszköz képességeiből adódó határokat a hardver vonatkozásában (4. ábra), amely a rádió maximális mintavételi frekvenciájából adódó felbontási korlát volt.

4. ábra: Bal oldalon egy monitoron látható tesztkép, jobb oldalon az RTL-SDR szoftverrádióval visszaállított kép
Forrás: a szerző felvételei

A valós idejű feldolgozás egyik eredménye a nem szándékosan kisugárzott monitorkép felderítésével kapcsolatos folyamatok kialakítása. Bár jelenleg nem automatizált a módszer, mégis leírható folyamatok mentén, aminek szerves része a szinkronjelek időtartományban történő vizsgálata, illetve azok korrelációjának megjelenítése. Ezzel a módszerrel egy folyamatos, az RTL-SDR teljes vételi tartományában végrehajtott szkenneléssel felderíthetők a kompromittáló frekvenciák.

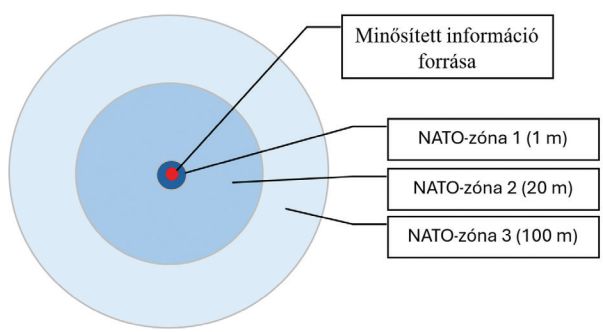
Másik eredményem a szoftverrádió korlátjainak meghatározása a visszaállított kép minőségének vonatkozásában. A közeg, a környezet és az eszközök jellegéből adódóan egy folyamatos, természetéből adódóan változó intenzitású zaj van jelen a visszaállított képen. Mivel ezen zavaró frekvenciák pixelszinten véletlenszerűen jelentkeznek, egyszerű átlagolással kiszűrhetők, ezzel jelentősen javítva a visszaállított kép minőségét. Jelen kutatás során a képek átlagolásán túl nem alkalmaztam a képminőség javítását célzó egyéb jelfeldolgozási eljárást. Bár az átlagolás hatékony megoldás, a visszaállított kép horizontális és vertikális futását a rádió feszültségvezérelt oszcillátorának hőmérsékleti stabilitása határozza meg. Az RTL-SDR esetében ezen alkatrész stabilitása csupán néhány képkockányi átlagolást tesz lehetővé. A folyamatos csúszásából eredendően a hosszabb átlagolások miatt elmosódottá válik a visszaállított kép.

A képminőség javítására további lehetőség a több vivőfrekvencián demodulált információ súlyozott összegzése,[11] illetve szoftveres jel- és képfeldolgozó algoritmusok, gépi tanulásos módszerek alkalmazása.

Felderíthetőség elleni védekezés

Védelem vonatkozásában a passzív TEMPEST-támadással szemben a minősítésnek megfelelő védőtávolság, illetve a körültekintő elektronikai tervezés jelenthet megoldást.

Ezeket az alapelveket már a második világháború végén is alkalmazták az USA híradó szervezetei, akkor a védőtávolságot 100, majd később 200 lábban határozták meg. Jelenleg Magyarországon a NATO SDIP-27 szerint szükséges a minősítésnek megfelelő zónákat meghatározni (5. ábra).[12]



5. ábra: Objektumon belüli védőtávolságok
Forrás: a szerző szerkesztése* SHOPINA *2020: 985 alapján

[11] KITAZAWA et al. 2022.
[12] SHOPINA 2020.

A védőzónák meghatározásán túl a veszélyeztetett eszköz gondos elektronikai tervezése jelenti az első védvonalat. Tervezéskor az EMC (*electromagnetic compliance* – elektromágneses megfelelőség) irányelveket érdemes szem előtt tartani, mivel a TEMPEST esetében is beszélhetünk kisugárzott, illetve a táp-, valamint vezetékes kommunikációs, illetve földelési vonalakon megjelenő nem kívánt információtartalomról. Fontos megjegyezni, hogy bár az elektromágneses vonatkozásban az EMC és a TEMPEST lényegüket tekintve azonosnak tűnhetnek, a két megfelelőség eltérő direktívák mentén működik.[13]

Az EMC kizárólag energiaszintekkel foglalkozik, a TEMPEST esetében viszont a kisugárzás információtartalmán van a hangsúly. Tehát ha van egy nagyintenzitású jelünk, ami miatt eszközünk nem teljesíti az EMC-megfelelőséget, ugyanakkor erre a nagyintenzitású jelre nincs érzékeny információt hordozó jel modulálva, a TEMPEST-megfelelőség teljesülhet az adott eszköz vonatkozásában. Másik esetet vizsgálva azonban, ha egy zavarjel megfelel az EMC-kritériumoknak, ugyanakkor intenzitása a TEMPEST-határvonalat túllépi, és védett információt tartalmaz, értelemszerűen beavatkozást tesz szükségessé a kiszivárgott jel intenzitásának csökkentése érdekében.

Ezen a ponton nem mindig jelentenek közvetlen megoldást az EMC-problémákkal kapcsolatos zajcsillapítási technikák. Jó példa erre az árnyékolás, amely bár hatékony az elektromágneses kisugárzások csillapításában, az árnyékolás kialakításának jellege, a tápellátás és egyéb áramköri megoldások, mint például az eszközök ESD- (*electrostatic discharge* – elektrosztatikus kisülés) védelme átalakíthatja a szivárgási csatornát kisugárzottról a vezetettre, amely elektronikai szempontból nehezebben kezelhető.[14]

Összegzés

Az információvédelem rendkívül szerteágazó terület, ahol a hatékonyság alapfeltétele a folyamatos kutatás és fejlesztés, hiszen az újabb technológiák hatékony kihasználásához megfelelő technikai megoldások is szükségesek. Kutatásom célja az volt, hogy bemutassam, a kereskedelmi forgalomban jelenleg bárki számára elérhető technológiák és technikai eszközök hatékony alkalmazásával belátható időtávon és költségvetéssel képessé válhatunk olyan minőségű berendezést előállítani, amely akár az oldalsávi elektromágneses kisugárzásból információ felderítésére és visszaállítására is alkalmas lehet. Éppen ezért tartom különösen fontosnak, hogy azokat az eljárásokat és irányelveket, amelyek mentén az eszközgyártók és az alkalmazók hatékonyan védekezhetnek az ilyen felderítési és lehallgatási eljárásokkal szemben, a lehető legkomolyabban vegyük figyelembe. Emellett rendkívül fontosnak tartom az ide vonatkozó jogszabályok frissítését, hazai TEMPEST-megfelelőségi kritériumok kidolgozását, illetve a polgári lakosság jövőbeni érintettségének vizsgálatát.

[13] Kinugawa–Fujimoto–Hajashi 2019.
[14] Pennesi–Sebastani 2005: 777–778.

Felhasznált irodalom

Eck, Wim Van (1985): Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk. *Computers & Security,* 4(4), 269–286. Online: https://doi.org/10.1016/0167-4048(85)90046-X

Kinugawa, Masahiro – Fujimoto, Daisuke – Hayashi, Yuichi (2019): Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure. *IACR Transactions on Cryptographic Hardware and Embedded Systems,* 2019(4), 62–90. Online: https://doi.org/10.46586/tches.v2019.i4.62-90

Kitazawa, Taiki et al. (2022): *TEMPEST Attack Against High-Resolution Displays Using Differences in the Transfer Function of EM Waves.* 2022 3rd URSI Atlantic and Asia Pacific Radio Science Meeting (AT-AP-RASC), Gran Canaria, Spain, 1–4. Online: https://doi.org/10.23919/AT-AP-RASC54737.2022.9814293

Kuhn, Markus G. (2003): *Compromising Emanations: Eavesdropping Risks of Computer Displays.* Technical Report 577. Cambridge: University of Cambridge. Online: www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf

Kuhn, Markus G. (2005): Electromagnetic Eavesdropping Risks of Flat-Panel Displays. In Martin, D. – Serjantov, A. (szerk.): *Privacy Enhancing Technologies.* PET 2004. Lecture Notes in Computer Science, 3424. Berlin–Heidelberg: Springer, 88–107. Online: https://doi.org/10.1007/11423409_7

Kuhn, Markus G. – Anderson, Ross J. (1998): Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. In Aucsmith, David (szerk.): *Information Hiding*. Lecture Notes in Computer Science, 1525. Berlin–Heidelberg: Springer, 124–142. Online: https://doi.org/10.1007/3-540-49380-8_10

Kuris Zoltán (2010): A komplex információvédelem új irányai a nemzeti minősített adatok védelmével összefüggésben. *Hadmérnök,* 5(4), 182–200. Online: https://real.mtak.hu/40796/

Marinov, Martin (2014): *Remote Video Eavesdropping Using a Software-Defined Radio Platform.* Cambridge: University of Cambridge.

National Security Agency (NSA) titkosítás alól feloldott *Tempest: A signal problem* című anyaga (1972). Online: www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf

Nemzeti Biztonsági Felügyelet (NBF): *TEMPEST*. Online: www.nbf.hu/hasznos-informaciok/tempest/

Pennesi S. – Sebastiani S. (2005): *Information Security and Emissions Control.* 2005 International Symposium on Electromagnetic Compatibility, Chicago, IL, USA, 777–781. Vol. 3. Online: https://doi.org/10.1109/ISEMC.2005.1513629

Shopina, Iryna et al. (2020): Cybersecurity: Legal and Organizational Support in Leading Countries, NATO and EU Standards. *Journal of Security and Sustainability,* 9, 977–992. Online: https://doi.org/10.9770/jssi.2020.9.3(22)