BERKI Gábor

AZ ELEKTRONIKAI VÉDELEM INFORMATIKAI ASPEKTUSAI

Napjainkra az elektronikai információbiztonság központi témává vált. A tanulmány az elektronikai hadviselés egyik fontos alkotóelemének, az elektronikai védelemnek számítógépekre, számítógép-hálózatokra alkalmazható elveit mutatja be. A számítástechnikai eszközök is bocsájtanak ki olyan elektromágneses sugárzásokat, amelyek illetéktelenek által történő rögzítése veszélyt jelenthet az elektronikai információbiztonságra. Bemutatom, hogyan, milyen módszerekkel rögzíthetők ezek a jelek, majd szólok az ez elleni védekezés kérdéseiről. Vázolom a TEMPEST szabványt, az ennek használatáról szóló jogszabályokat és az elektronikai pusztítás elleni védelem lehetőségeit. Ismertetem ezek helyét a Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrínájában. Bemutatom azt a koncepciót, amelyet az Egyesült Államok hadseregének 2014 februárjában kiadott, a kiber elektromágneses tevékenységekkel foglalkozó, FM 3-38-as utasítása tartalmaz.

Kulcsszavak: elektronikai hadviselés, információbiztonság, TEMPEST

IT ASPECTS OF ELECTRONIC PROTECTION

Nowadays the importance of electronic information security is rapidly growing and it became a widely discussed topic in the last decade. This article intends to explain the PC network applicable principles of electronic protection, which is one of the most important parts of electronic warfare. Computer technology devices emit electromagnetic radiation, which, if recorded by unauthorized persons, can threaten electronic information security. I try to explain how these signs can be recorded and present the protection methods. I briefly outline the TEMPEST standard, the legal background of its use and the alternatives of protection against electronic destruction also pointing them out in the Hungarian Defence Forces' Joint Forces Electronic Warfare Doctrine. I explain the concept described in the FM 3-38 manual on cyber electromagnetic activities issued by the US Army in February 2014.

Keywords: electronic warfare, information security, TEMPEST

Bevezetés

A XXI. század vitathatatlanul az információs társadalom kora. A XX. század végén hihetetlenül felgyorsult a mikroelektronika fejlődése, ez a számítástechnika és az információfeldolgozás sosem látott térhódításához vezetett. Napjainkra az ipart, a bankszektort, a kereskedelmet, de bátran kijelenthetjük, hogy az élet minden területét átszövik a számítógépes hálózatok, hatékony működésük ezek nélkül már elképzelhetetlen lenne.

Az államgépezetek, a védelmi szektor és a hadseregek is komoly függésbe kerültek az informatikai hálózatoktól, tehát ezek védelme, működésük biztosítása elsőrendű feladattá vált a fejlett világban. Ha megfordítjuk ezt a tételt, akkor tehát azt is kijelenthetjük, hogy ha egy konfliktus során sikerül a szemben álló fél informatikai, elektronikai rendszereinek működésében zavart okoznunk, ezzel komoly előnyre tehetünk szert. Az ezt a képességet lehetővé tevő elektronikai, illetve számítógép-hálózati hadviselés tehát egyre nagyobb jelentőséggel bír a konfliktusokban, napjaink hadviselésében. Jelen tanulmányban azt kívánom bemutatni, hogy az elektronikai védelemnek milyen informatikai aspektusai vannak, tehát hogy milyen módon érinti az informatikai biztonságot. Véleményem szerint két területet kell megvizsgálnom. Elsőként a felderítés elleni tevékenységet, amely szoros kapcsolatban áll az információbiztonsággal és az elektronikai pusztítás elleni védelmet, amely az informatikai berendezések működőképességének megőrzését érinti.

Az elektronikai védelem helye, szerepe

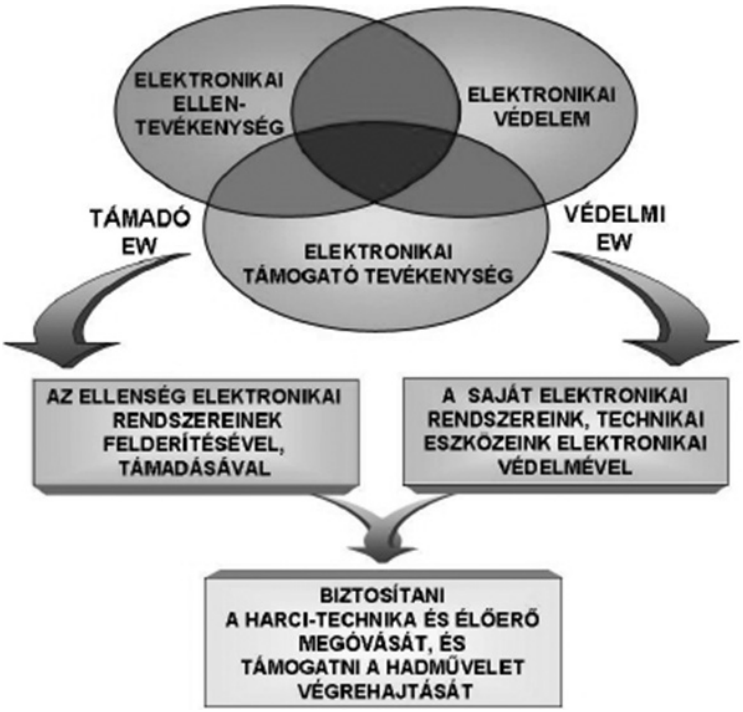
A modern háborúk már elképzelhetetlenek elektronikai hadviselés nélkül, hiszen a harc sikeres megvívásához nélkülözhetetlen felderítési adatok megszerzése és az ellenség felderítésének akadályozása kulcsfontosságú tényező. Az elektronikai védelem az elektronikai hadviselés egyik alkotóeleme. A Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrínája szerint:

„Az elektronikai hadviselés az EM-spektrumot hasznosító azon katonai tevékenység, amely magába foglalja az elektromágneses kisugárzások kutatását, felfedését és azonosítását, az irányított energiát is beleértve az elektromágneses energia felhasználását abból a célból, hogy megakadályozza vagy korlátozza az ellenség részéről az EM-spektrum hatékony használatát, és lehetővé tegye annak a saját csapatok általi használhatóságát." [1]

Mint ahogy azt az 1. ábra szemlélteti, ennek három, egymást átfedő területe van:

- elektronikai támogató tevékenység;
- elektronikai ellentevékenység és
- elektronikai védelem.

Célja az ellenség katonai információs rendszereiben működő elektronikai eszközök elektronikai úton való felfedése, azonosítása, támadása, illetve a saját rendszerek működőképességének megóvása.



1. ábra: Az elektronikai hadviselés területei (forrás: [2])

Mivel a téma szempontjából az első két terület nem releváns, ezért ezek bemutatásától jelen írásban eltekintek.

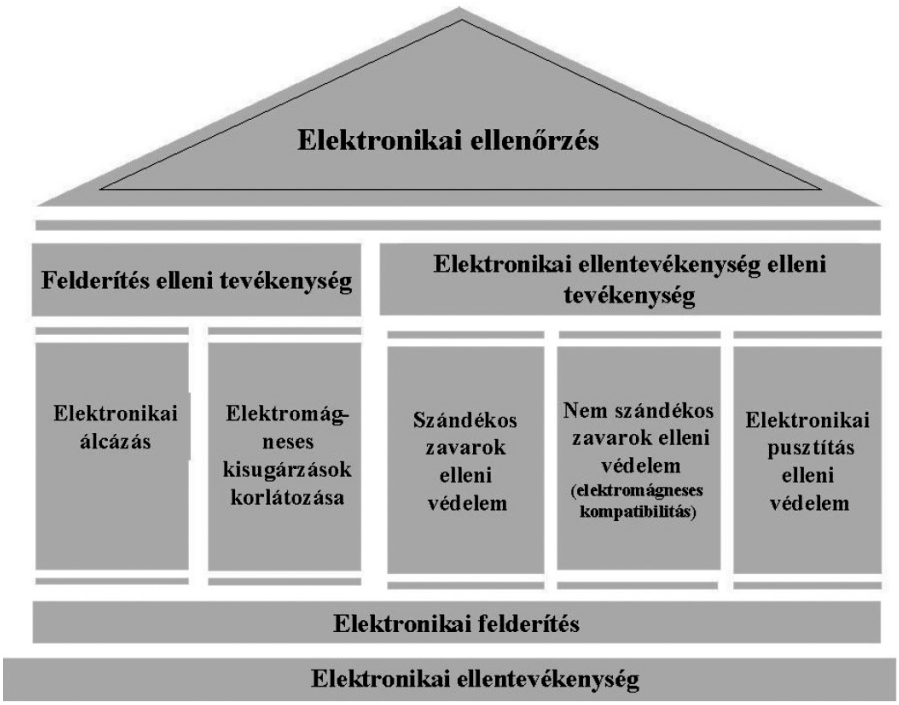
Az elektronikai védelem az elektronikai hadviselés azon része, amely biztosítja az elektromágneses spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok nem szándékos elektromágneses interferenciái ellenére. Az elektronikai védelmi tevékenységek védelmi természetűek.

Az elektronikai védelem alapvetően három fő területre osztható fel, úgymint:

- az elektronikai felderítés elleni tevékenység;
- az elektronikai ellentevékenység elleni tevékenység és
- az elektronikai ellenőrzés.

Megvalósításához passzív és aktív rendszabályokat kell meghatározni az elektronikai eszközök és rendszerek működése számára, megfelelő kiképzéssel magas fokú jártasságot kell kifejleszteni a kezelőszemélyzet körében az ellenséges elektronikai hadviselési környezetben történő üzemeltetésre. A passzív elektronikai védelmi rendszabályok között kell megemlíteni a kisugárzási korlátozások alkalmazását, a rövid idejű, csökkentett teljesítményű kisugárzásokat, az irányított antennák használatát, valamint a kezelési utasításokban foglaltak pontos betartását és betartatását. Az aktív rendszabályok közé tartozik az adóberendezések paramétereinek – frekvencia, modulációs mód, teljesítmény – változtatása. [3]

A felderítés elleni tevékenység magában foglalja az elektromágneses kisugárzások korlátozását és a felderítés előli kitérés különböző módozatait. Az elektronikai ellentevékenység elleni tevékenységhez a szándékos és a nem szándékos elektromágneses zavarok elleni tevékenységek, továbbá az elektronikai pusztítás elleni védelem tartozik. Az elektronikai ellenőrzés pedig az előzőekben említett két fő terület rendszabályai betartásának ellenőrzését foglalja magában. Ugyanakkor az elektronikai védelem sikeres megvalósítása megköveteli a szoros együttműködést az elektronikai hadviselés más összetevőivel is.



2. ábra: Az elektronikai védelem területei (forrás: [2])

A felderítés elleni tevékenység

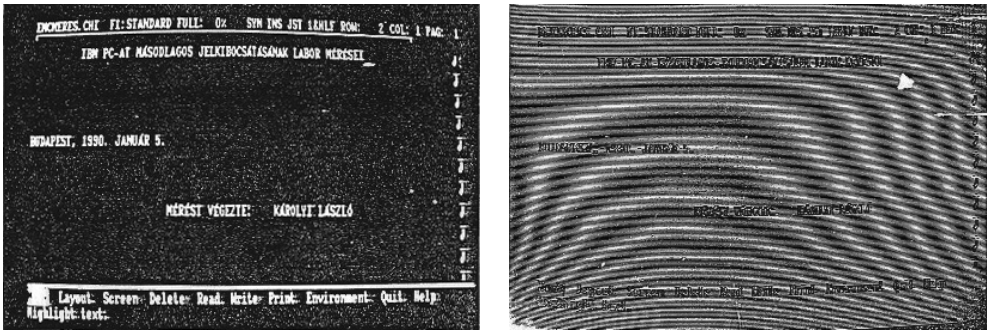
A felderítés elleni tevékenység célja, hogy megakadályozzuk az ellenérdekelt felet abban, hogy felderítési adatokat gyűjtsön. Ezt többek között az ellenséges felderítő berendezések zavarásával, elektronikai álcázással, illetve a saját elektromágneses kisugárzások korlátozásával érhetjük el. [2] Azonban nem felejtkezhetünk meg azokról az ellenséges felderítés számára jelentőséggel bíró kisugárzásokról sem, amelyet a saját készülékeink bocsájtanak ki működésük közben. A digitális berendezések áramköreinek működésekor rádiófrekvenciás tartományba eső kisugárzások is keletkeznek. Ezek a sugárzások többféleképpen terjedhetnek:

- Primer sugárzásként. Ilyenkor a gerjesztett vezeték antennaként működve elektromágneses teret hoz létre maga körül.
- Szekunder sugárzásként, a környezetben lévő fémtárgyak felszínén végigfutó felületi hullámok formájában.
- A hálózati tápegység modulációival. [4]

Egy megfelelően hangolt vevőberendezéssel ezek a sugárzások felfoghatóak, és belőlük olyan adatok nyerhetők ki, amelyek veszélyeztethetik az információbiztonságot. A számítógépes hardver minden egyes alkatrésze kibocsát nem kívánt jeleket, azonban ezeknek csak egy része igazán veszélyes. A komoly problémát azok a pontok jelentik, ahol soros adatfeldolgozás, adattovábbítás történik. Sugárzási szempontból a leginkább védtelenek a monitorok és a soros kábelek. A PC-k monitorainak szinkronjeleinek a megfelelő berendezéssel történő rekonstruálásával a megjelenő kép a „távolban" visszaállítható.

1991-ben Károlyi László *Az információvédelem biztonságát növelő, műszaki-kriptoanalitikai támadási módszerek elleni defenzió* című doktori értekezésében bebizonyította, hogy egy megfelelően összeállított vevőegység képes a távolból egy IMB PC-kompatibilis számítógép monitorának nem szándékos kisugárzásai alapján rekonstruálni a képernyő tartalmát. Megállapította, hogy elsősorban a 20–40 Mhz-es, illetve a 60–150 MHz-es tartományban végzett mérésekkel lehetséges értékelhető jeleket fogni. Az ennél alacsonyabb frekvenciákon a rossz antennahatásfok, a két tartomány között pedig a környezeti zajok miatt nem keletkeztek értékelhető adatok. [4] A kísérlet eredményét az alábbiakban láthatjuk: jobb oldalt az eredeti képernyőkép, bal oldalt pedig az ellenőrző monitor képe.

A mérőantennák és a számítógép közötti távolság 30 méter volt. Mint az látható, az ellenőrző monitoron felismerhető és olvasható az eredeti képernyőtartalom. A monitorok kompromittáló kisugárzásának vizsgálatáról világszerte számos publikáció látott már napvilágot. A lehallgatás módszeréről 1985-ben egy holland informatikus, Wim van Eck adott ki publikációt. A szakiroda-



3. ábra: Az eredeti és a helyreállított kép (forrás: [4])

lom azóta nevezi ezt a tevékenységet „Van Eck phreaking”-nek. De példaképpen Marcus Kuhnnak, a cambridge-i egyetem kutatójának munkáit is meg kell említeni, aki már az LCD-monitorok lehallgathatóságát kutatta.

Nem kívánatos kisugárzása azonban nem csak a monitoroknak van. A Lausenne-i Műszaki Egyetem biztonsági és kriptográfiai laboratóriumában végzett vizsgálatok azt mutatták, hogy mind a vezetékes, mind a vezeték nélküli billentyűzetek könnyűszerrel lehallgathatók, az általuk kibocsájtott jelek egy megfelelő antenna és vevőegység segítségével felfoghatók és dekódolhatók. A tizenkét vizsgált billentyűzet (hét PS2, 2 USB, 3 vezeték nélküli) mindegyikét sikerült lehallgatni a négy vizsgálati módszer legalább egyikével. [5]

A probléma tehát nem új keletű. A számítógépes hardver elektromágneses kisugárzása és ezáltal a lehallgathatósága már az 1960-as években felmerült. Az amerikai NSA[1] az 1970-es években TEMPEST[2] néven programot indított a probléma vizsgálatára; amely a keretét adta a későbbi, az elektromágneses lehallgatás ellen védett készülékek tervezésére és gyártására vonatkozó TEMPEST-szabványoknak.

A probléma megoldásához tehát ellenintézkedéseket kell hozni, amelyek olyan szintre csökkentik a berendezések által kibocsájtott jelek energiáját, amelyek már nem teszik lehetővé, hogy azokat bármely ellenérdekelt fél detektálja és analizálja.

Ehhez a berendezéseket megfelelő tanúsítványok szerint szintekbe sorolják a kisugárzásuk erőssége szerint. A szinteket a következő módon jelölik:

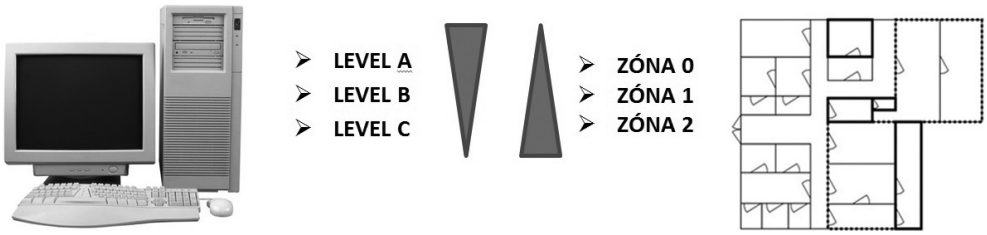
- LEVEL A
- LEVEL B
- LEVEL C

[1] National Security Agency.
[2] Transient Electromagnetic Pulse Emanation Standard.

A berendezések üzemeltetésére szolgáló helyiségeket a közterületektől való távolságuk és jelcsillapítási képességeik szerint zónákra osztják, a következő módon:

- ZÓNA 0
- ZÓNA 1
- ZÓNA 2

Ezek után az alábbi ábra szerinti illesztést kell megvalósítani. [6]



4. ábra: A TEMPEST szintjeinek és a zónáinak illesztése (forrás: saját készítés)

Értelemszerűen a magasabb jelkibocsájtással rendelkező berendezések kerülhetnek a közterületektől távolabb eső, védettebb helyiségekbe és fordítva. A helyiségek kialakításakor is figyelemmel kell lenni bizonyos védőtávolságok betartására a szekunder sugárzások kialakulásának megakadályozására. A legjobb megoldás természetesen egy tökéletesen árnyékolt helyiség létrehozása, ez azonban a magas költségek miatt általában nem kivitelezhető. A lehallgatások elleni védelem még egy módszere, ha a berendezés sugárzási frekvenciáján, az adott hullámsávokon egy kis teljesítményű adóval fehér zajt gerjesztünk. Ez meggátolhatja a lehallgatást.

Maga a TEMPEST-szabvány nem nyilvános, így a konkrét számadatok sem, de a megfelelő engedélyekkel rendelkező eszközgyártók és építési kivitelezők természetesen rendelkeznek a szükséges információkkal. A szabványokat a következő dokumentumokban fektették le:

SDIP-27: NATO TEMPEST követelmények és kiértékelési eljárásrend

SDIP-28: NATO zónázási eljárásrend

SDIP-29: Létesítmények tervezésére és minősített információt feldolgozó eszközök telepítésére vonatkozó követelmények

SDIP-30: Minősített információt feldolgozó elektronikai eszközök telepítésére vonatkozó követelmények

AC/322-D(2007)0036: INFOSEC technikai és alkalmazási direktíva a kisugárzás biztonságáról

Hazánkban *a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól* szóló 161/2010. (V. 6.) kormányrendelet foglalkozik azokkal a kérdésekkel,

amelyek a TEMPEST-et érintik. A jogszabály a Nemzeti Biztonsági Felügyeletet jelöli meg az alábbi feladatok végrehajtására:

„a) a kompromittáló kisugárzás elleni védelem tekintetében felügyeletet és ellenőrzést gyakorol,

b) meghatározza és a minősített adatkezelést végző szervek részére elérhetővé teszi a TEMPEST biztonsági követelményeket,

c) ellenőrzi a rendszer és működési környezete TEMPEST megfelelőségét,

d) TEMPEST vizsgálatokat, méréseket végez vagy végeztet,

e) a TEMPEST mérések alapján határozatot ad ki az eszközök besorolására, valamint a rendszer környezetének zónabesorolására vonatkozóan,

f) a TEMPEST biztonság veszélyeztetése esetén a rendszer használatát korlátozhatja, megtilthatja, a szerv vezetőjét a kompromittáló kisugárzás elleni védelem helyreállítása érdekében szükséges intézkedések megtételére kötelezheti, a kiadott rendszerengedélyt visszavonhatja.” [7]

Azok a szervezetek, amelyek minősített adatokkal dolgoznak, kérhetik a felügyelet vizsgálatát, amely mobil zónázó mérőkészlet segítségével helyszíni felmérést készít az elektronikus minősített adat kezelésre kijelölt helyiségről és annak környezetéről. A mérési adatok és szabványok alapján kerül sor a zónába sorolásra, majd a hatósági határozat kiadására. A kérelemben többek között a helyszínrajzot, az alaprajzot, a biztonsági rendszerek elemeit, a különböző csatlakozók és gépészeti berendezések elhelyezését is meg kell adni. [8]

A fentiek alapján tehát elmondhatjuk, hogy az információt feldolgozó berendezések lehallgathatóságának védelme a megfelelő szabványok, előírások betartásával, illetve a megfelelő berendezések használatával megoldható.

Az elektronikai pusztítás elleni védelem

A másik témakör, amely az elektronikai védelem informatikai aspektusához tartozik, az elektronikai pusztítás elleni védelem.

Az elektronikai pusztítás az elektromágneses és egyéb irányított energiák alkalmazása az ellenség elektromágneses spektrum használatán alapuló rendszereinek időleges vagy tartós rombolása céljából. Eszközei közé tartozik a nukleáris robbanás elektromágneses impulzusa, a nagy energiájú rádiófrekvenciás sugárforrások és az impulzusbombák. [2]

Napjainkban minden elektronikai eszközben integrált áramkörök, félvezetők tucatjai találhatók. Egy nagy energiájú elektromágneses impulzus hirtelen felhevíti ezeket, és mivel képtelenek ezt a hőt elvezetni, összeolvadnak, ezzel gyakorlatilag működésképtelenné válnak. A hatvanas évek elején a Szovjetunióban egy hidrogénbomba robbantásakor vették észre, hogy a rob-

banás több száz kilométer távolságban tönkretette a kommunikációs berendezéseket. A jelenséget később amerikai tudósok is megfigyelték hidrogénbomba-kísérletek során.

Az impulzusbombák lényege, hogy vegyi robbanóanyag robbantási energiáját alakítják elektromos energiává egy üregrezonátor és tölcsérsugárzó segítségével. A megfelelő magasságban robbantott e-bomba közel kör alakú területen fejti ki pusztító hatását az elektronikai eszközökkel szemben. Használatuk elsősorban az ellenséges erők vezetési pontjai, kommunikációs központjai ellen lehet hatásos egy összecsapás során.

Könnyen belátható, hogy egy ilyen típusú támadás az informatikai eszközökre végzetes hatással járhat. Az ellenük való védekezés több módon is megvalósítható. A rádiófrekvenciás energiát elnyelő, ún. abszorbeáló anyagok alkalmazásával történő árnyékolás meglehetősen drága és bonyolult, inkább csak speciális épületeknél használatos. A reflektáló árnyékolási módszernél olyan bevonatot képeznek a védendő felületen, amelyen keresztül a támadó elektronikai sugárzás csak erősen csillapítva jut át. [2]

A leghatásosabb védekezési módszer azonban a Faraday-kalitka, amely egy olyan zárt teret alkot, ahol a teret határoló elemek elektromágneses vezető anyagból állnak, így a külső elektromágneses tér nem lesz hatással a belsejére. A határolók vezetőképessége nem szakadhat meg a nyílászáróknál és a felületek találkozásánál sem. Megfelelő szűréssel kell ellátni a térbe belépő energiaellátó és kommunikációs vezetékeket is. Ezzel a módszerrel szervertermeket, számítógépközpontokat is meg lehet védeni az elektromágneses hullámok ellen.

Az elkövetkezendő években fel kell készülni az ilyen típusú támadásokra is, főleg, hogy a technológia fejlődésével könnyebben előállíthatóvá válnak ezek a típusú fegyverek, és tartok tőle, hogy a nemzetközi terrorizmus is fel fogja fedezni a bennük lévő lehetőségeket, hisz a segítségükkel könnyen indítható komoly következményekkel járó támadás.

Összegzés

Az informatikai biztonság három alapvető eleme a bizalom, a sértetlenség és a rendelkezésre állás. Ez azt jelenti, hogy az adatokat csak az ismerhesse meg, akire tartozik, ne lehessen rajtuk rossz szándékú módosítást végrehajtani és hogy a szükséges helyen és időben hozzáférhetőek legyenek. [9] Cikkemben azt kívántam összefoglalni, hogy az elektronikai védelemnek milyen, az informatikával, az informatikai biztonsággal kapcsolatos aspektusai vannak. Két területet vizsgáltam meg, amely hatással van az informatikai rendszerekre és az informatikai biztonságra. A felderítés elleni tevékenység,

amellyel azt akadályozzuk meg, hogy az ellenség elektromágneses kisugárzásaink elemzésével információkhoz juthasson, a bizalmasság védelmét valósíthatja meg, míg az elektronikai pusztítás elleni védelem a rendelkezésre állás elvét. Ez is mutatja, hogy informatikai rendszereinket nemcsak a számítógép-hálózati műveletek ellen kell felkészítenünk, hanem az elektronikai hadviselés ellen is.

Irodalomjegyzék

[1] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína. Honvéd Vezérkar Felderítő Csoportfőnökség, 2005. MH DSZFT kód: 11216.
[2] HAIG Zsolt – KOVÁCS László – VÁNYA László – VASS Sándor: *Elektronikai hadviselés.* Nemzeti Közszolgálati Egyetem, Budapest, 2014, ISBN 978-615-530587-0
[3] HAIG Zsolt – VÁRHEGYI István: *Hadviselés az információs hadszíntéren.* Zrínyi Kiadó, Budapest, 2005, ISBN 963 327 391 9
[4] KÁROLYI László: *Az információvédelem biztonságát növelő, műszaki-kriptoanalitikai támadási módszerek elleni defenzió.* Egyetemi doktori értekezés, 1991.
[5] Martin VUAGNOUX – Sylvain PASINI: *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards,* http://infoscience.epfl.ch/record/140523/files/VP09.pdf (letöltve: 2014. 09. 29.)
[6] *TEMPEST introduction.* A Secure Systems & Technologies Ltd. honlapja, www.sst.ws/downloads/TEMPEST%20Introduction%20iss%203.pdf (letöltve: 2014. 09. 29.)
[7] 161/2010. (V. 6.) kormányrendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól
[8] A Nemzeti Biztonsági felügyelet honlapja, www.nbf.hu/tempestmer.html (letöltve: 2014. 10. 09.)
[9] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. *Bolyai Szemle,* 2008, XVII. (4), 137–156.