HADMÉRNÖK

IV. Évfolyam 2. szám - 2009. június

Kuris Zoltán
Igazságügyi és Rendészeti Minisztérium
kurisz@irm.gov.hu

Pándi Erik
Zrínyi Miklós Nemzetvédelmi Egyetem
pandi.erik@zmne.hu

KOMPLEX INFORMÁCIÓBIZTONSÁG MEGVALÓSÍTÁSI LEHETŐSÉGEINEK MEGKÖZELÍTÉSE

Absztrakt

Jelen közleményben a szerzők kifejtik a fizikai biztonság, személyi biztonság és dokumentáció biztonságról kialakult nézeteket, kutatási eredményeket. A publikáció egy olyan vállalkozás ipari kémkedés elleni védelmének információbiztonsági követelményeit tekinti át, amely egyúttal NATO beszállítói státusszal is rendelkezik.

This paper introduces scientific results of physical security, personal security, document security and information security. The publication examines information security requirements against economic intelligence of an Enterprise that is licensed for NATO's supply status.

Kulcsszavak: *biztonság, dokumentum biztonság, információ, információbiztonság, információs rendszer, fizikai biztonság, személyi biztonság, védelem*

BEVEZETÉS

A jogosulatlan információgyűjtés során a törvénytelen megfigyelésre vonatkozó bizonyítékok a nyilvánosság kizárása miatt jellemzően elhallgatásra kerülnek. Sok szervezetnek, gazdálkodó egységnek nincs is tudomása arról, hogy az ipari kémkedés mennyiben befolyásolja mindennapi tevékenységének számos spektrumát. Nyilvánvalóan az üzleti szférán túlmenően az állami, ezen belül a védelmi szektoron belül is fontos az, hogy a minősített, vagy stratégiailag fontos információ ne juthasson illetéktelen személyek tudomására. Az információbiztonságot alapvetően rendszerként szemlélhetjük, amelynek keretében az összetevőket alrendszereként definiálhatjuk. Tesszük ezt azért, mert véleményünk szerint az ipari kémkedés, jogosulatlan információgyűjtés elleni védekezés akkor és csak is akkor hatékony, ha az *információvédelem* alrendszerei komplex módon kerülnek megszervezésre, alkalmazásra és működése rendszeresen ellenőrizhető. Természetesen az újonnan felmerülő kockázati tényezőket figyelembe véve,

időközönként megfelelő kockázatelemzés elkészítése után a védelem újraszervezése elkerülhetetlen.

Megítélésünk szerint, a témakört érintően, a releváns jogszabályi környezet az alábbiak szerint azonosítható be és foglalható össze:

- az államtitokról és szolgálati titokról szóló 1995. évi LXV. törvény;
- a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény;
- a Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvény;
- az elektronikus aláírásról szóló 2001. évi XXXV. törvény;
- a rejtjeltevékenységről szóló 43/1994. (III.29.) Korm. rendelet;
- a minősített adat kezelésének rendjéről szóló 79/1995. (VI.30.) Korm. rendelet;
- a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól szóló 179/2003. (XI.5.) Korm. rendelet;
- a Nemzeti Biztonsági Felügyelet részletes feladatairól és működési rendjéről, valamint az iparbiztonsági ellenőrzések részletes szabályairól szóló 180/2003. (XI.5.) Korm. rendelet.

A felsorolt szabályozási háttér felhasználása révén a következőkben az ipari kémkedés elleni védelem információbiztonsági követelmények egyes kérdéseit tekintjük át.

1. AZ INFORMÁCIÓVÉDELEM ALAPVETŐ KÉRDÉSEI

A témakör elvi feldolgozása során mindenképpen szükségszerű néhány alapkérdés áttekintése, illetőleg belső tartalmának megvilágítása.

1.1. Az információ védendő tulajdonságai

- bizalmasság (az információhoz csak a jogosultsággal rendelkezőnek férhet hozzá);
- hitelesség (az információ azon jellemzője, amely az eredetiséget reprezentálja);
- rendelkezésre állás (az arra jogosultak a működési szabályzatban meghatározottak szerint férnek hozzá az információhoz);
- sértetlenség (a megfelelő módon működő információs rendszer az adatokat megfelelő formában reprezentálja).

1.2. A védeni kívánt információk megjelenési formái

- adathordozón rögzített, továbbított minősített adat;
- írásos formában megjelenő információ, minősített adat;
- minősített információt hordozó objektum, technikai eszköz;
- nem tárgyiasult formában megjelenített minősített információ, eljárási mód, ismeretanyag;
- szóban közölt minősített információ.

1.3. Fizikai biztonság

Minden olyan gazdálkodó szervezetnek, amely NATO minősített[1] információkat kíván kezelni, illetve tárolni helyi NATO Nyilvántartót kell kialakítania. A Nyilvántartó létesítése érdekében a kérelmező gazdálkodó szervezet írásbeli megkereséssel fordul a Nemzeti Biztonsági Felügyelethez (Felügyelet). A kérelem alapján a Felügyelet helyszíni szemlét hajt végre, és meghatározza a megfelelő szintű fizikai biztonság kialakítása érdekében teendő valamennyi intézkedést. Fontos hangsúlyozni, hogy a helyszíni szemle végrehajtása kötelező. Az eljárás eredménye alapján a gazdálkodó szervezetnek el kell készítenie a Nyilvántartó sematikus helyszínrajzát.[2] A helyszínrajzot a Felügyelet hagyja jóvá, ez alapján kezdődhet meg a Nyilvántartó kialakítása. A következőkben a Nyilvántartó kialakításához szükséges szempontokat tekintjük át, azonban lényeges itt megemlítenünk, hogy egységes, *„zsinórmértékszerű”* követelmények meghatározására lényegében nincs lehetőség, hiszen a fizikai környezet mindenütt eltérő. A fizikai védelem az alábbi gondolatok köré csoportosítható:

- az objektumok felderítés elleni védelme;
- az objektumokba történő belépés- és benntartózkodás rendje;
- technikailag biztonságos területek, és kompromittáló kisugárzásoktól védett zónák kialakítása;
- a minősített információk kezelésére szolgáló területek védelme. Ezen belül megvédeni az információkat az erővel, vagy lopva történő behatolás ellen. A biztonságos tárolás, raktározás biztosítása.

A fizikai biztonság tekintetében a biztonsági területek felosztása lényegében hármas tagozódást mutat, úgymint **I. osztályú biztonsági terület**, **II. osztályú biztonsági terület**, valamint **adminisztratív zóna**.

A Nyilvántartó területén NATO minősített adatok mindhárom zónában tárolhatók. Az I. osztályú biztonsági terület olyan terület, ahol NATO CONFIDENTIAL vagy annál magasabb minősítésű információt dolgoznak, fel vagy tárolnak olyan módon, hogy a területre való belépés, a minősített információkhoz való hozzáférést is jelenti egyben. A II. osztályú biztonsági területen NATO CONFIDENTIAL vagy annál magasabb minősítésű információt dolgoznak, fel vagy tárolnak úgy, hogy a jogosulatlan hozzáférést belső ellenőrzéseken keresztül lehet megakadályozni. Az adminisztratív zónába a belépés ellenőrzött és regisztrált (elektronikus beléptetéssel), illetőleg a területen belül a személyek és járművek mozgása ellenőrizhető.

A Nyilvántartó **Feldolgozó** és **Tároló** helyiségből áll. A Tároló helyiség egy, vagy több helyiségből állhat. A Feldolgozó helyiség lehet egy vagy több helyiség, iroda, épületrész vagy teljes épület. A Tároló helyiség csak a Feldolgozó helyiséggel szomszédos terület lehet.

A Feldolgozó helyiségbe a be- és kiléptetés csak regisztrált és ellenőrzött beléptetést biztosító elektronikus beléptető rendszeren keresztül történhet. A Feldolgozó helyiség falazatának, födémének és padozatának meg kell felelnie a 30 cm vastagságú tömör téglafal szilárdsági mutatójának. A Feldolgozó helyiség ajtaja a Magyar Biztosítók Szövetsége (MABISZ) által kiállított érvényes Biztosítói Minősítési Tanúsítvánnyal (Tanúsítvány) rendelkező, NATO SECRET jelölésű adatok esetén minimum 10 perces, NATO CONFIDENTIAL jelölésű adatok esetén minimum 5 perces áthatolási, áttörési ellenállásra képes biztonsági ajtónak kell

[1] NATO RESTRICTED, NATO CONFIDENTIAL, NATO SECRET

[2] Ezen csak a falak típusát, vastagságát, a telepített biztonságtechnikai eszközök (érzékelők, biztonsági ajtó lemezszekrény stb.) helyét és típusát kell feltüntetni

lennie. A biztonsági ajtót minden esetben nyitásérzékelővel kell ellátni. A Feldolgozó helyiségbe mozgásérzékelőt és füstérzékelőt kell felszerelni. Csak olyan elektronikai jelzőrendszer telepíthető, melynek alkotóelemei érvényes MABISZ Tanúsítvánnyal rendelkeznek és a teljes körű elektronikai jelzőrendszer alkotóelemeivel szemben támasztott követelményeknek, megfelelnek. Amennyiben a Feldolgozó helyiségben ablakok találhatók, úgy a következő fizikai méretű fix, illetve nyitható belső ráccsal[3] kell ellátni:

- NATO SECRET jelölésű adatok esetén 90x90 mm-es kiosztású, 10 mm átmérőjű köracélból álló, minden pontján hegesztetett rácsszerkezet;
- NATO CONFIDENTIAL jelölésű adatok esetén 140x140 mm-es kiosztású, 10 mm átmérőjű köracélból álló, minden pontján hegesztetett rácsszerkezet.

A Tároló helyiségbe a be- és kiléptetés csak regisztrált és ellenőrzött beléptetést biztosító beléptető rendszeren keresztül történhet. A Tároló helyiség falazatának, födémének és padozatának meg kell felelnie a 30 cm vastagságú tömör téglafal szilárdsági mutatójának, kivéve a Tároló és a Feldolgozó helyiség közötti falat, mely bármilyen válaszfal lehet. A Tároló helyiség ajtaja bármilyen ajtó lehet. A tároló helyiség ajtaját minden esetben nyitásérzékelővel kell ellátni. A Tároló helyiségbe mozgásérzékelőt és füstérzékelőt kell telepíteni. Csak olyan elektronikai jelzőrendszer telepíthető, melynek alkotóelemei érvényes MABISZ Tanúsítvánnyal rendelkeznek és a teljes körű elektronikai jelzőrendszer alkotóelemeivel szemben támasztott követelményeknek, megfelelnek.

A NATO minősített adatok tárolására szolgáló, MABISZ tanúsítvánnyal rendelkező mechanikus számkombinációs zárral is ellátott **tároló eszközt** a Tároló helyiségben kell helyezni.

A Nyilvántartó riasztó központja jelzéseinek vagy az épület őrzés-védelmét ellátó szervezethez, vagy a rendőrségre kell befutnia. A reagálás módját írásban kell rögzíteni. A biztonsági tárolóeszközök **kulcsait** az épületből kivinni nem lehet. Ezek tartalékpéldányát és a **kódokat** a biztonsági megbízott őrzi – *a tárolt adatok minősítési szintjének megfelelő* – tárolóeszközben. A reagáló erők a kulcsokhoz nem férhetnek hozzá. A kulcsok felvétele, illetve leadása dokumentált módon, az erre a célra nyitott átadókönyvben történhet. Minden számkombinációt külön borítékba kell elhelyezni. A számkombinációt meg kell változtatni:

- a berendezés használójának változásakor;
- a számkombináció felfedése, vagy annak veszélye esetén;
- de legalább minden év elteltével.

A **fizikai védelem** célja tehát nem más, minthogy egyrészt lehetővé váljon a személyi állomány szétválasztása a NATO minősített információkhoz való hozzáférés kapcsán a *„csak azoknak, akiknek szükséges tudni róla”*[4] elv alapján. Másodrészt a jogosulatlan személyek illetéktelen, vagy erőszakos behatolása meghiúsuljon. Harmadrészt a hűtlen személyek (a beépített kémek) tevékenységének elrettentése, megakadályozása és felfedése, illetőleg – *utolsóként* – ha titoksértés történik, minél előbb felfedésre kerülhessen. A fizikai biztonság kialakításakor figyelembe kell venni:

- a hozzáférők körének személyi biztonsági szintjét;

[3] nem kell rácsszerkezetet alkalmazni, amennyiben a talajszint feletti magasság a 6,5 métert meghaladja és egyéb veszélyeztető tényező nem merül fel. Nyitható rácsszerkezet esetén mechanikus számkombinációs zárat kell felszerelni. Az ablakokra minden esetben nyitásérzékelőt kell felszerelni.
[4] need to know

- helyi biztonsági környezetet;
- az információ minősítési szintjét;
- az információ mennyiségét és formátumát;
- az információ tárolásának kívánt módját.

1.4. Személyi biztonság

Az eljárásrendnek biztosítania kell, hogy a személyek megbízhatóak legyenek és megfeleljenek a biztonsági kritériumoknak. A külföldi minősítéssel és jelöléssel ellátott adatokhoz a hozzáférés csak azon személyek számára engedélyezhető, aki átesett a 1995. évi CXXV. törvény 71. § (2) bek. b) pontjában meghatározott szintű ellenőrzésen, kockázati tényező személyükkel kapcsolatban nem merült fel, a külföldi minősítéssel és jelöléssel ellátott adatok ismerete állami vagy közfeladat végrehajtásához szükséges, és rendelkeznek az erre vonatkozó, a Felügyelet által nyilvántartásba vett Személyi Biztonsági Tanúsítvánnyal és az erről szóló Igazolással. A Személyi Biztonsági Tanúsítvány nyilvántartásba vételét a kezdeményező szerv biztonsági megbízottja a 180/2003. (XI.5.) Korm. rendelet 1. számú mellékletében szereplő Adatlap kitöltésével kérelmezi a Felügyelettől. A Személyi Biztonsági Tanúsítvány nyilvántartásba vételéhez a kérelmező az Adatlapot megküldi a Felügyelet részére. A kérelmező felelőssége, hogy csak olyan személy részére kérje Személyi Biztonsági Tanúsítvány nyilvántartásba vételét, akinek a külföldi minősítéssel és jelöléssel ellátott adat megismerése, illetve kezelése állami vagy közfeladat végrehajtásához szükséges. A Felügyelet nyilvántartásba veszi a Személyi Biztonsági Tanúsítványt és kiadja az erről szóló igazolást. Az igazolást a kérelmező szervhez továbbítja, melyet a biztonsági megbízott köteles kezelni.

Abban az esetben, ha Személyi Biztonsági Tanúsítvánnyal rendelkező személy tekintetében az előzőekben meghatározott feltételek a továbbiakban nem állnak fenn, az érintett szerv biztonsági megbízottja a Felügyeletet haladéktalanul értesíti, amely a Személyi Biztonsági Tanúsítványt visszavonja. A biztonsági megbízott az igazolást jegyzőkönyv felvétele mellett megsemmisíti. Abban az esetben, ha a Felügyelet közvetlenül szerez tudomást arról, hogy a Személyi Biztonsági Tanúsítvánnyal rendelkező személy tekintetében a fentiekben meghatározott feltételek a továbbiakban nem állnak fenn, a Felügyelet a Személyi Biztonsági Tanúsítványt visszavonja, és ennek tényéről tájékoztatja a kérelmezőt. A biztonsági megbízott az Igazolást jegyzőkönyv felvétele mellett megsemmisíti. További elvárások:

- a Személyi Biztonsági Tanúsítványok nem másolhatóak;
- az érintett személynek a Személyi Biztonsági Tanúsítványon kívül betekintési engedéllyel és titoktartási nyilatkozattal is rendelkeznie kell, ez utóbbi két dokumentum nem semmisíthető meg;
- amennyiben valamely személynek a NATO minősített információkhoz történő hozzáférési jogosultsága megszűnik (pl.: felmondás, új munkakör stb.) a Felügyeletet a Személyi Biztonsági Tanúsítvány visszavonása érdekében írásban azonnal értesíteni kell.

1.5. Dokumentáció biztonság

Ahhoz, hogy a Nyilvántartó a szükséges Engedélyét megkapja, teljesíteni kell a NATO minősített információk kezeléséhez (nyilvántartásához) szükséges valamennyi dokumentum (adminisztratív) biztonsági feltételt is, vagyis fel kell készülni a NATO minősített információk fogadására. Ezek teljesítése érdekében a Nyilvántartónak rendelkeznie kell valamennyi nyil-

vántartási segédlettel.[5] Ezekre vonatkozó minták a minta csomagban megtalálhatók. A dokumentum biztonság részletes szabályait a 179/2003. (XI.5.) Korm. rendelet tartalmazza. A fentieken kívül szükséges a Biztonsági Szabályzat[6] és a Vészhelyzeti Intézkedési Terv kidolgozása is. A folyamat vége maga az akkreditálás, melynek során a Felügyelet ellenőrzi:

- a kialakított Nyilvántartó fizikai biztonsági követelményének érvényesülését;
- az érintett személyek Személyi Biztonsági Tanúsítványának, betekintési engedélyének, titoktartási nyilatkozatának meglétét;
- a Biztonsági Szabályzat, valamint a Vészhelyzeti Intézkedési Terv meglétét és alkalmazhatóságát;
- a nyilvántartási segédletek hiteles felfektetését.

1.6. Az információs társadalom infokommunikációs rendszerei elleni fenyegetések

A teljes körű információbiztonság megvalósításának, a *„végtelen biztonságnak”* végtele ára is van, hiszen mindig fennállhat úgynevezett maradék kockázat. Ahhoz, hogy a jogosulatlan technikai információszerzés esélyét minimalizáljuk, megfelelően hatékony védelmi intézkedéseket kell foganatosítani. Az intézkedések egy változatban az alábbiak szerint csoportosíthatók:

1.6.1. Megelőző technikai védelmi intézkedések

Ezen kategóriába sorolhatjuk a védett tárgyalók, irodák védelemtechnikai kialakítását. Az informatikai (vezetékes és vezeték nélküli) hálózatvédelmi tevékenységet, a személyi számítógépek kisugárzás védelmét (TEMPEST), az ablakok lehallgatás gátló védőfóliával való ellátását, valamint az adat és távbeszélő rejtjelzés különböző eszközeinek alkalmazását. A védett tér kialakításával szemben támasztott követelmények:

- elhelyezés (a védett helyiség közvetlen közelében lehetőség szerint csak könnyen ellenőrizhető helyiség legyen);
- védelem (a helyiségben önálló, csak a helyiség védelmét szolgáló beléptető és behatolás jelző rendszert kell alkalmazni, állandó felügyelettel. A helyiségbe való beléptetés proximity kártyával, és PIN kóddal történhet. Az autonóm riasztó és beléptető központ fémháza a helyiségen belül, kulccsal zárható rádiófrekvenciásan nem árnyékoló szekrényben kerül elhelyezésre. A védett helyiséget mozgásérzékelővel, üvegtörés érzékelővel és a nyílászárókat nyitásérzékelővel kell ellátni. A használaton kívüli védett helyiség riasztórendszere mindig élesítettnek kell lennie);
- kábelezés (a védett tárgyaló belső elektromos csövezéseiben lehetőleg ne legyenek az épület egyéb elektromos vezetékei. A védett tárgyalóban csak a szükséges elektromos és kommunikációs kábelezés legyen. Ezeket a kábeleket süllyesztett kivitelben kell szerelni. A helyiségbe számítógép és távbeszélő hálózat kiépítése nem javasolt. Az esetleges kommunikációt szükség szerint DECT telefon alkalmazásával kell biztosítani. A védett térbe belépő erősáramú kábel a helyiségen kívülről, egy a tárgyaló külső falán elhelyezett, zárható kapcsolószekrényből induljon. A 230 V-os hálózatot fázisonként a szekrényben elhelyezett kismegszakítóval, és külön ere a célra készített 100 Hz-es alul áteresztő szűrővel kell ellátni. A tárgyalóból az összesített riasztás jelzés

[5] főnyilvántartó könyvvel, iktatókönyvvel (külön minősítési szintenként), átadókönyvvel, stb.
[6] amely a gazdálkodó szervezet tekintetében a részletes személyi-, fizikai- és dokumentum biztonsági feltételeket tartalmazza

egy érpáron érkezik. A helyiségen kívülre jól látható helyre, csak a behatolás jelző kezelőjét és a beléptetéshez szükséges kártyaolvasót kell kábelezni).

A kialakítás egyéb szempontjainak figyelembe vétele során a védett helyiséget el kell látni elektromágneses árnyékolással. Az ablakokat információvédelmi fóliával kell szerelni. Az elektronikus eszközök számát minimalizálni kell. A padlózat ne legyen álpadló és a falak, nem lehetnek lambériával ellátva. A padlózatba és a mennyezetbe akusztikus rezgetőket kell beépíteni 2 m²-enkét egyet-egyet. A bejárati ajtó hangszigetelt legyen, és elektromos zárral kell ellátni. Falon kívüli technológiával szerelt világítás alkalmazása javasolt. A védett helyiségben a tárgyalás ideje alatt működnek az akusztikus rezgetők, valamint működik a 900 MHz-es, az 1800 MHz-es GSM, a 3G, WiFi és bluethot eszközök blokkolására alkalmas több sávos blokkoló rendszer. A védett téren belül csak speciális (titkosított rögzítésre alkalmas) konferencia rendszer üzemelhet.

1.6.2. Előzetes technikai átvizsgálás

A védett teret időszakosan és igénybe vétel előtt közvetlenül, előzetes technikai átvizsgálásnak kell alávetni. A technikai átvizsgálás kiterjed a hangfrekvenciás, rádiófrekvenciás, távbeszélő és erősáramú (vivőfrekvenciás), valamint infra tartományban működő jogosulatlan információgyűjtő eszközök (hang és kép) felderítésére. A felderítés hatékonyságának növelése érdekében különböző specifikus és komplex tartomány vizsgálatára alkalmas felderítő eszközöket (detektorokat) kell használni. Megítélésünk szerint megfelelőnek a megjelenítési, naplózási és dokumentációs funkciókkal is rendelkező eszköz tekinthető.

1.6.3. Technika átvizsgálás beléptetéskor

Adott esetben, különböző tárgyalások és rendezvények alkalmával a védett térbe való belépéskor technikai átvizsgálást szükséges végrehajtani. Ebben a fázisban szűrhető ki azon (hang és kép felvételére alkalmas) eszközök, melyeket a meghívottak, a technikai személyzet tagjai juttathatnak a védett térbe. A hangosítás eszközeit különös figyelemmel kell átvizsgálni. A védett téren belül hangosításra rádiós mikrofont alkalmazása nem engedhető meg.

1.6.4. Valós idejű eszközök alkalmazása

A védett térben elhangzottak rádiófrekvenciás lehallgatásának megakadályozása érdekében a tárgyalás ideje alatt online eszközök alkalmazásával adatok gyűjthetők. Érzékelhetővé válnak a kisugárzott jelek, iránymméréssel megállapítható a kisugárzás pontos helye is.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Közleményünkben igyekeztünk lényegre törően érzékeltetni a jogosulatlan információgyűjtés elleni védekezés kérdéseit. Az információbiztonságot alapvetően rendszerként szemléltük, amelynek keretében az összetevőket alrendszereként definiáltuk. Tettük ezt azért, mert véleményünk szerint az ipari kémkedés, jogosulatlan információgyűjtés elleni védekezés akkor és csak is akkor hatékony, ha az *információvédelem* alrendszerei komplex módon kerülnek megszervezésre, alkalmazásra, illetőleg működésük folyamatosan ellenőrzésre.

A szakirodalomra, a jogszabályokban foglaltakra, valamint gyakorlati tapasztalatainkra építve áttekintettük a fizikai-, személyi- és dokumentumbiztonsági alrendszerek főbb jellemzőit, konkrét esetre alapozva a megvalósításra tettünk javaslatokat. Az általunk kifejtett technikai

szaktevékenységek megítélésünk szerint az információs társadalomban egyre nagyobb létjogosultságot szerez, hiszen ha a teljes rendszer jól felkészült információvédelmi szakemberek alkalmazásával és megfelelő technológia bevetésével kerül aktiválásra, akkor az *„információs hadviselés”* területén hatékonyan alkalmazható rendszer épült ki.

Meggyőződésünk, hogy az újkori konfliktusok kezdete nem a különféle csapatmozgásokban nyilvánul meg elsődlegesen, hanem az információs társadalom kritikus infrastruktúráit érő támadások tekinthetők kezdeti jeleknek. Ezért tartottuk fontosnak kihangsúlyozni, hogy a támadások ellen megfelelő ellentevékenységek végrehajtásával kell védekezni, ellenben az egyes közfeladatot ellátó, vagy gazdálkodó szervezet vissza nem fordítható, és felbecsülhetetlen károkat szenvedhet.

Felhasznált irodalom:

[1] Dr. Haig Zsolt: Az információbiztonság komplex értelmezése, ZMNE

[2] http://www.intpro.co.uk/oscor.htm, letöltve: 2009. 01.25.

[3] http://www.securifocus.com/portal.php?pagename=fo01_Inf_infrastruktúrák.ppt ; 1. fog

[4] http://www.research-electronics.com/cgi-bin/main.cgi?action=viewprod&ct=products&pct

=ORION&num=NJE-4000, letöltve: 2008. 12.12.

[5] http://www.tscm.com/reioscor.html, letöltve: 2009.01.14.

[6] Dr. Kovács László: Információs terrorizmus, HDI konf., ISSN 1417-7323, 128-137. o.

[7] Dr. Lukács György, Gábor László: Új vagyonvédelmi nagykönyv