DR. HAIG ZSOLT

AZ INFORMÁCIÓS TÁRSADALOM INFORMÁCIÓBIZTONSÁGA[1]

INFORMATION SECURITY OF INFORMATION SOCIETY

A cikk bemutatja az információs társadalom sebezhetőségét, értelmezi a kritikus információs infrastruktúrákat és kihangsúlyozza a komplex információbiztonság szükségességét.

This paper introduces the vulnerability of the information society, interprets the critical information infrastructures, and emphasises the necessity of complex information security.

Bevezetés

Napjainkban az információs társadalom egyik legjelentősebb kihívása a biztonság megteremtése, amely túlmutat az eddig ismert biztonságfelfogás dimenzióin. A klasszikus biztonságdimenziók, mint a politikai-, gazdasági-, katonai-, környezeti- és a társadalmi dimenzió, mellet az információs társadalom biztonságos működtetése szükségessé teszi egy újabb biztonsági dimenzió, az információbiztonság értelmezését. Mivel az információs társadalom működése elképzelhetetlen az információtechnológia alkalmazása és az infokommunikációs rendszerek működése nélkül, így azok természetszerűleg jelen vannak a politikai, gazdasági, katonai és társadalmi életben. Ennek megfelelően az információbiztonság az előbb említett biztonságdimenziókat átfogó tényezővé vált. Az információbiztonság ma már nem egyszerűen egy vírusirtó szoftver vagy egy tűzfal alkalmazását jelenti. Ennél többre van szükség, ha a társadalom működését szavatolni akarjuk. Átfogó és komplex szabályozásra, egyértelmű feladatrendszerrel rendelkező információbiztonsági szervezetekre és az emberek tudatos felkészítésére.

[1] Jelen írás az MTA Bolyai János Kutatási Ösztöndíjának támogatásával készült

1. Információs társadalom

Az információs társadalom új típusú társadalmi alakulat, amely az ipari társadalom utóda. Emiatt posztindusztriális társadalomnak is nevezik. Az információs társadalom kialakulását az elektronika és az informatika rohamos fejlődése gerjesztette. Az infokommunikációs technológiák és a hálózatok egyre növekvő hatása az egyén, a társadalom, a gazdaság és a kultúra területén egyaránt jelentkezik. Az infokommunikációs hálózatok gazdag eszköz- és szolgáltatásválasztékot kínálnak, befolyással vannak az egyén, a társadalom, a gazdaság és a kultúra viselkedésére, működésére, megváltoztatják a munkavégzés, tanulás, szórakozás formáit. Az információs társadalomban a munka tárgya, a társadalom működésének mozgatórugója nem az anyag és az energia, hanem az információ. [1]

Az információ és a tudás meghatározóvá válása a tudomány eredményeinek intenzív és folyamatos felhasználását eredményezi, ami miatt korunk társadalmát ezért tudástársadalomnak is szokás nevezni.

Az infokommunikációs hálózatok átalakítják a társadalmi kapcsolatokat. A felgyorsult modern életmód fellazítja vagy akár felbontja az olyan korábbi megszokott társadalmi közösségeket, mint a család, a lakóhelyi, munkahelyi és szakmai közösségek. Az új technológia és azok szolgáltatásai viszont új, alapvetően hálózatos elven létrejövő és működő közösségeket hoz létre. Az infokommunikációs hálózatok mindinkább a társadalom új kapcsolati eszközévé válnak, és az emberek, csoportok is egyre inkább hálózatos elven szerveződnek. [1]

Az információs társadalom ultrafejlett, szabad piacgazdaságú, demokratikus elvű és globális kiterjedésű kapitalizmus. Hálózatos kapcsolatai révén gyors, pontos döntések meghozatalát biztosító, a köz– és magánügyeket távolból intézhető távtársadalom. [2]

Az információs társadalom globális, szabadpiacú, parlamenti demokráciára épülő, ultrafejlett kapitalista gazdasági rendszer, amelynek középpontjában az információ, a tudás és a tudomány áll, és működését az infokommunikációs hálózatok biztosítják. E társadalomban szélessávú infokommunikációs hálózatokra épülő kormányzati, önkormányzati, közigazgatási és védelmi intézményrendszerek működnek, ahol a közügyeket, vállalati és magánügyeket az információs közműhálózaton (információs infrastruktúrán) keresztül közvetlen (on-line) hozzáféréssel távolból lehet intézni. A fejlett infokommunikációs hálózatok révén az informáci-

ók megszerzése, feldolgozása, és a megalapozott döntések meghozatala és továbbítása terén a világ és az eddigi történelem leggyorsabb társadalma. [3]

Az infokommunikációs hálózatok lehetővé teszik az állam számára a hatékony és olcsó működést. Az infokommunikációs technológia révén az egyén és az állam, valamint a gazdálkodó szervezetek és az állam kapcsolata fokozatosan új alapokra kerül. A hálózatok által az egyének és a közösségek közvetlenül vehetnek részt a helyi, térségi és országos közügyek intézésében és a döntéshozatalban. [4]

Magyarország a '90-es évek közepén felismerte az információs társadalom építésében rejlő lehetőségeket, és megtette a kezdeti lépéseket annak érdekében, hogy felzárkózzunk az Európai Unió által elvárt szintre. Ennek fontos állomásai a távközlési piac liberalizációja, a szélessávú internet hozzáférés egyre szélesebb körben való lehetővé tétele, és az információs társadalom építésének irányvonalát meghatározó stratégiák kidolgozása. [2]

A 2003-ban kiadott Magyar Információs Társadalom Stratégia egyértelműen megfogalmazza, hogy „A tudásalapú gazdaság és információs társadalom létrehozásával a legfőbb közös cél az egyén és a közösség életminőségének és életkörülményének javítása; ennek révén olyan modern, európai, magyar köztársaság megteremtése, amelyben mindenkinek jó élni. Ezt a célt a XXI. században a tudásteremtés- és terjesztés, a gazdasági versenyképesség, a közösségvállalás, a társadalmi esélyegyenlőség a nemzeti kulturális és természeti környezet megőrzésének értékei mentén lehet a legbiztosabban és a leggyorsabban elérni." [5: 11.p] Ugyanakkor azt is leszögezi, hogy a legnagyobb kihívás a fejlett infokommunikációs technológiák széleskörű alkalmazása, amelynek révén lehetővé válik a gazdaság és a társadalom modernizációja, versenyképességének növelése és felzárkózás az európai tudástársadalmak élmezőnyébe. [5]

Az információs társadalomban a kormányzat új kihívásokkal kerül szembe:

- törvényekkel kell támogatni az elektronikus kereskedelmet, az online üzleti tevékenységet, a jogi és adminisztratív ügyek elektronikus intézésének lehetőségét és jogszerűségét;

[2] Nemzeti Információs Társadalom stratégia (2001); Magyar Információs Társadalom Stratégia (2003)

- a kormányzati és közigazgatási szolgáltatásokat elektronikusan is hozzáférhetővé kell tenni (e-kormányzás, e-közigazgatás) és
- az embereket fel kell készíteni az infokommunikációs technológiák alkalmazására és a rájuk épülő szolgáltatások hasznosítására. [4]

2. Az információs táradalom sebezhetősége

Az információs társadalom nagyon fejlett, nagyon hatékony társadalom, ugyanakkor meglehetősen sebezhető is. Sebezhetőségének alapját az adja, hogy működése szorosan kapcsolódik a globális, nemzeti, regionális és lokális információs környezethez. Ennek következtében igen erősen függ az információs környezet fejlett, ám erősen korlátozható, vagy sebezhető integrált információs infrastruktúráitól, mint pl. a távközlési hálózatoktól és a számítógép-hálózatoktól. Az információs társadalom hatalmas teljesítményekre képes a tudomány, a termelés, az információcsere és a távolból intézhető ügyek területén. Ugyanakkor ennek a jelentős teljesítménynek vannak árnyoldalai is, amelyek üzemzavarból, szándékos rongálásból, károkozásból vagy pusztításból eredhetnek. Egy olyan bonyolult, informatikailag behálózott társadalomban és gazdaságban, ahol közel minden ügyünket a hálózaton keresztül intézünk, saját fejlettségünk csapdájába eshetünk (lásd a 2007. májusi Észtország elleni DDoS[3] típusú hálózati támadást). Ezt a rossz szándékú egyének, csoportok, bűnözők, terroristák is jól tudják, és mindent elkövetnek annak érdekében, hogy az információs társadalom felgyorsult és lüktető életritmusát korlátozzák, vagy átmenetileg beszüntessék.

Az infokommunikációs hálózatok célpontjai is és egyben eszközei is mind a nemzetközi terrorizmusnak, mind az elektronikus bűnözésnek. Az információs infrastruktúrák elleni komplex információs támadások, mint az információs hadviselés, információs műveletek a katonai, gazdasági, politikai célú érdekérvényesítés új, komplex formájává váltak. Az információs társadalom ezen árnyoldalát már számos fejlett országban felismerték, és komolyan elemezték, vizsgálták, hogy mi történik abban az esetben, ha valamilyen ártó szándékú szervezet fizikai, vagy információs csapást mér a társadalom működtetéséért felelős információs infrastruktú-

[3] DDoD — Distributed Denial of Service (megosztott szolgáltatás-megtagadással járó támadás)

rákra. Több szimulációs gyakorlaton[4] különböző fajtájú információs és fizikai támadásokat intéztek az integrált infokommunikációs rendszerek ellen, és azt vizsgálták, hogy a támadás következtében azok milyen károkat szenvedhetnek el.

Az információs és fizikai támadások totálisan (polgári és katonai célpontok ellen egyaránt) összpontosított módon (kiemelt célcsoportok ellen) vagy szelektív formában (egyes kritikus infrastruktúrák ellen) történhetnek. Szinte mindegyik gyakorlat végső konklúziója az volt, hogy ilyen típusú támadásokkal egy hálózatilag fejlett ország társadalmi, politikai, gazdasági és védelmi rendszere erősen befolyásolható, korlátozható.

A komplex információs támadások következtében az ország vezetése, tőzsdei és bankrendszere, pénzügyi élete, földi, légi, tengeri közlekedése, energiahordozó- és ellátó rendszerei, élelmiszerellátása stb. megbénulnak vagy erősen akadoznak. Az egészségügyi ellátás leáll, a közbiztonság felbomlik, az addigi szervezett rend káosszá változik. [2]

Egy ország információs infrastruktúráin keresztüli sebezhetőségét a katonai vezetők is felismerték. Az első és második Öböl-háború illetve a boszniai és afganisztáni harci tapasztalatok azt bizonyítják, hogy az információs műveleteken belüli komplex információs támadásokkal jelentős mértékben tudták támogatni a harcoló erőket. Kiderült, hogy az ellenség információs rendszereinek és ellátó infrastruktúráinak információs támadásával jelentős mértékben csökkent az ellenség vezetésének hatékonysága és eredményessége. A támadások célpontjai az alábbiak voltak:

- villamos energetikai rendszerek: erőművek, transzformátor állomások, távvezeték rendszerek;
- közműhálózati információs rendszerek: víz-, gáz-, olaj-, benzinellátás, raktárközpontok;
- szállítási rendszerek: diszpécserhálózatok, közúti, vasúti, légi, belvízi és tengeri hajózási, személy- és teherszállítási rendszerek;
- hadászati vezetési információs infrastruktúrák: katonai és polgári távközlési és vezetési rendszerek, számítógép-hálózatok, vezetési pontok;
- légvédelmi információs infrastruktúrák: radarállomások, rakéta–indítóállások, légvédelmi parancsnoki harcálláspontok;

[4] Pl. az USA Belbiztonsági Minisztériuma által szponzorált Cyber Storm II. National Cyber Exercise 2008 májusában

- légierő információs infrastruktúrák: repülőterek, légierő navigációs berendezései, radarállomások, levegő-levegő, levegő-föld összeköttetések, légierő földi irányító pontjai, légi vezetési pontok;
- haditengerészeti információs infrastruktúrák: kikötők, navigációs rendszerek, hajó-hajó, hajó-szárazföld összeköttetések;
- szárazföldi haderő információs infrastruktúrái: felderítő rendszerek, vezetési rendszerek, információs műveletekben alkalmazható rendszerek;
- média: országos tájékoztató rendszerek, rádió-műsorszóró és TV-adóállomások, stúdiók, szerkesztőségek, távközlési és adatátviteli hálózatok. [2]

A fenti infrastruktúrák, infokommunikációs rendszerek elleni támadások a hatásalapú műveletek[5] keretében zajlottak. A katonai műveletekben alkalmazott hatásalapú megközelítés elve szerint a hadszíntéren egymással hálózatba kapcsolt objektumok, központok találhatók, amelyek egymással alá- és fölérendeltségi viszonyban állnak. Ez lehetőséget nyújt arra, hogy egy kiválasztott központ és a benne található nagyfontosságú célpontok elleni támadás különböző hatásokat eredményezzen a többi, hozzájuk kapcsolódó központ, objektum működésében is. Mindez igaz a polgári létesítményekre, infrastruktúrákra is, amelyek — az információs társadalom alapelvéből fakadóan — az infokommunikációs hálózatokon keresztül szintén szoros kapcsolatban állnak egymással. Tehát bármely fontos, kritikus információs infrastruktúra illetve annak eleme elleni információs vagy fizikai támadás további működésbeli korlátokat idézhet elő a többi, hozzá kapcsolódó infrastruktúrában, rendszerben is.

3. Kritikus információs infrastruktúrák

Amikor az új típusú társadalmi berendezkedésről és annak biztonságos működtetéséről beszélünk, akkor nemzetbiztonsági szempontból mindenképpen ki kell emelnünk az un. kritikus infrastruktúrákat, amelyek működése az információs társadalom szempontjából létfontosságú. Amennyiben ezek valamilyen beavatkozás, vagy természeti katasztrófa következtében működésképtelenné vagy működésükben korlátozottá válnak, annak beláthatatlan következményei lehetnek az ország biztonságára, gaz-

[5] Effect Based Operations

dasági és védelmi képességeire. Ezért a kritikus infrastruktúrák ismerete és pontos behatárolása létfontosságú, mivel — az információs rendszereiken keresztül — fokozottan ki vannak téve egy információs támadásnak, így azok potenciális célpontok lehetnek. [2]

Az elmúlt években több példa is rámutatott a kritikus infrastruktúrák sebezhetőségére és védelmének szükségességére. Elég, ha csak a különböző természeti katasztrófákra (földrengések, szökőár), terrorcselekményekre (World Trade Center, madridi vonatrobbantás, londoni metrórobbantás) gondolunk. A védelem megvalósítása érdekében több ország és nemzetközi szervezet is kidolgozta erre vonatkozó koncepcióját[6].

Magyarország e téren is megkezdte a felzárkózást: a terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004 (V.7.) Korm. határozat és a módosításáról szóló 2046/2007 (III.19.) Korm. határozat már foglalkozik a kritikus infrastruktúrák védelmének kérdéseivel. A konkrétabb szabályozást az Európai Unió Zöld Könyvének figyelembevételével 2008-ban alkotta meg a kormány, amikor is kiadta a 2080/2008. (VI. 30.) Korm. határozatát a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. A határozat 1. melléklete (Zöld Könyv) részletesen meghatározza a kritikus infrastruktúra fogalmát, a szektorokat és a védelem feladatait.

A Zöld Könyv szerint „Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.

Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.” [6: 220.p]

[6] Pl.: Európai Unió COM (2004) 702; COM (2005) 576; COM (2006) 786

A Zöld Könyv a kritikus infrastruktúrák 10 ágazatát és 43 álágazatát különbözteti meg, úgymint:

1. „Energia (kőolaj kitermelés, finomítás, tárolás és elosztás; földgáztermelés, tárolás, szállítás és rendszerirányítás, elosztás; villamosenergia-termelés, átvitel és rendszerirányítás, elosztás);
2. Infokommunikációs technológiák (információs rendszerek és hálózatok; eszköz-, automatikai és ellenőrzési rendszerek; internet, infrastruktúra és hozzáférés; vezetékes és mobil távközlési szolgáltatások; rádiós távközlés és navigáció; műholdas távközlés és navigáció; műsorszórás; postai szolgáltatások; kormányzati informatikai, elektronikus hálózatok);
3. Közlekedés (közúti közlekedés; vasúti közlekedés; légi közlekedés; vízi közlekedés; logisztikai központok);
4. Víz (ivóvíz szolgáltatás; felszíni és felszín alatti vizek minőségének ellenőrzése; szennyvízelvezetés és –tisztítás; vízbázisok védelme; árvízi védművek, gátak);
5. Élelmiszer (élelmiszer előállítás; élelmiszer-biztonság);
6. Egészségügy (kórházi ellátás; mentésirányítás; egészségügyi tartalékok és vérkészletek; magas biztonsági szintű biológiai laboratóriumok; egészségbiztosítás);
7. Pénzügy (fizetési, értékpapírklíring- és elszámolási infrastruktúrák és rendszerek; bank és hitelintézeti biztonság);
8. Ipar (vegyi anyagok előállítása, tárolása és feldolgozása; veszélyes anyagok szállítása; veszélyes hulladékok kezelése és tárolása; nukleáris anyagok előállítása, tárolása, feldolgozása; nukleáris kutatóberendezések; hadiipari termelés; oltóanyag és gyógyszergyártás);
9. Jogrend - Kormányzat (kormányzati létesítmények, eszközök; közigazgatási szolgáltatások; igazságszolgáltatás);
10. Közbiztonság - Védelem (honvédelmi létesítmények, eszközök, hálózatok; rendvédelmi szervek infrastruktúrái).” [6 221.p]

A felsorolás alapján megállapítható, hogy a hazai Zöld Könyv illeszkedik az EU szabályozáshoz, hasonló kritikus infrastruktúra meghatározást alkalmaz, mint az EU ide vonatkozó szabályzója. [7] A dokumentum nem foglalkozik azonban a kritikus információs infrastruktúrák kérdésével. Tekintettel arra, hogy az információs infrastruktúrák alapvetően meghatározzák az információs társdalom zavartalan működését, feltétlenül értelmezni kell azokat. A kritikus infrastruktúrák védelmére vonatkozó euró-

pai programról szóló zöld könyv szerint: „Kritikus információs infrastruktúrák közé azok sorolandók, melyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, Internet, műholdak stb.)". [8]

A fentiek alapján a kritikus információs infrastruktúrák alatt az alábbiakat értelmezhetjük:

- energiaellátó rendszerek rendszerirányító infokommunikációs hálózatai;
- infokommunikációs hálózatok (vezetékes, mobil, műholdas);
- közlekedés szervezés és irányítás infokommunikációs hálózatai;
- vízellátást szabályzó infokommunikációs hálózatok;
- élelmiszerellátást szabályzó infokommunikációs hálózatok;
- egészségügyi rendszer infokommunikációs hálózatai;
- pénzügyi-gazdasági rendszer infokommunikációs hálózatai;
- ipari termelést irányító infokommunikációs hálózatok;
- kormányzati és önkormányzati szféra infokommunikációs hálózatai
- védelmi szféra infokommunikációs hálózatai.

Az információs társadalom információs infrastruktúráinak komplex rendszere egymásra épülő, egymást feltételező, egymást kölcsönösen támogató infrastruktúrák szövevényes hálózataiból tevődik össze. Ezt egymástól való függőségnek, interdependenciának nevezzük. Az összekapcsolódó infrastruktúrákon keresztül az esetleges üzemzavarból vagy szándékos támadásból fakadó problémák felhalmozódhatnak, váratlanabb és lényegesen súlyosabb működésbeli zavart okozhatnak az adott állam létfontosságú szolgáltatásaiban. Az infrastruktúrák összekapcsolódásai és egymástól való függőségei sérülékenyebbé teszi őket a különböző fizikai és információs támadásokkal szemben. [9]

Amennyiben az infrastruktúrarendszer bármely csoportját támadás éri, az közvetlenül vagy közvetve negatívan befolyásolja a másik működését is. A már korábban említett hatásalapú megközelítés elve is az interdependencia jelenségét használja ki.

Összességében kijelenthető, hogy az infrastruktúrák közötti kölcsönös függőség következtében:

- az információs társadalom szervezett információs és vezetési működési rendjére, minőségére, harmóniájára, dinamikus egyensúlyára;

- vezetési rendszerének hatékonyságára, a vezetés integrációjára, annak szilárdságára és minőségére;
- a vezetés struktúrájára, szervezettségi fokára;
- a belső és külső kommunikációra, a kapcsolati viszonyokra és végezetül;
- az adott szervezet operatív vezethetőségére igen komoly, negatív hatást lehet gyakorolni. [2]

4. Komplex információbiztonság kialakítása

A kritikus információs infrastruktúrák elleni fenyegetések a fizikai, az információs és a tudati dimenzióból egyaránt származhatnak[7]. Ez azt jelenti, hogy az információs infrastruktúrákat fenyegető támadások az alábbiak lehetnek:

- elektronikai felderítés (információs dimenzió);
- elektronikai támadás (információs dimenzió);
- számítógép-hálózati támadás (információs dimenzió);
- fizikai támadás (fizikai dimenzió). [11]

Az infrastruktúra a létesítményeken, eszközökön, berendezéseken kívül magában foglalja az azt működtető személyzetet, humán erőforrást is, ami szintén támadható pl. különböző pszichológiai hadviselési módszerekkel (tudati dimenzió).

Tekintettel a támadások formáira, az információs társadalom információbiztonsága azt jelenti, hogy a kritikus információs infrastruktúrák védelmét e három dimenzióban kell megvalósítani. A komplex információbiztonság tehát nem egyenlő az informatikai biztonsággal, annál jóval több és komplexebb, bonyolultabb tervezési, szervezési és végrehajtási folyamat.

Az információbiztonság összetettségét figyelembe véve megállapítható, hogy az nem csak technológiai kérdés, bár megteremtésében és fenntartásában jelentős szerepe van a különböző információvédelmi eszközöknek, eljárásoknak.

A 2003-as keltezésű Magyar Információs Társadalom Stratégiában megfogalmazásra került, hogy „a fejlett országok gyakorlatával ellentétben, az informatikai biztonság helyzetére hazánkban jellemző, hogy:

[7] Bővebb kifejtését lásd [10] irodalomban.

- súlya, kezelése nincs arányban a fontosságával
- nincs egységesen alkalmazott módszertan és
- nem kapcsolódik a fő nemzetközi áramlatokhoz." [5]

Sajnos azt kell látnunk, hogy ezek a problémák ma is többnyire léteznek, ezért az információbiztonság terén fennálló problémák veszélyeztethetik az állam- és közigazgatás működőképességét.

Széles körű együttműködésre van szükség ahhoz, hogy az emberek, a gazdasági szervezetek (vállalkozások) és a kormányzat bizalommal lehessenek az információs társadalom iránt. Ez sok esetben nehezen megvalósítható, hiszen egy paradoxont kell feloldani. Az információs társadalomhoz olyan fogalmak társulnak, mint az információszabadság, az információhoz való szabad hozzáférés, és működését szerteágazó, nem hierarchizált kapcsolatok jellemzik. Ezzel szemben az információbiztonság szigorú szabályozást (jogszabályok, szabványok, ajánlások), szervezett intézkedéseket, szervezett kereteket (információbiztonsági szervezetek) és magas fokú tudatosságot feltételez. E látszólag egymásnak ellentmondó fogalmaknak, intézkedéseknek, tevékenységeknek kell egymással harmonizálni, ahhoz, hogy az információs társadalmat biztonságosnak mondhassuk.

A kormányzat számára ezért kiemelt feladat az infokommunikációs hálózatokba vetett bizalom erősítése, az információbiztonsági tudatosság és ismeretek fejlesztése. A közszféra fontos feladata a jogi környezet megteremtése, a megfelelő szervezeti keretek kialakítása és saját rendszerén belül a szükséges technikai feltételek megvalósítása.

Összességében az információs társadalom komplex információbiztonságának kialakítása terén az alábbi fő feladatokat kell végrehajtani:

- komplex információbiztonsági (infokommunikációs biztonsági) stratégia kidolgozása és elfogadása;
- komplex információbiztonság jogszabályainak, szabályozói környezetének biztosítása;
- információbiztonsági követelmények kidolgozása, nemzetközi szabványok honosítása;
- komplex információbiztonsági szervezetek létrehozása, meglévő szervezetek feladatainak pontosítása, kibővítése az átfogó információbiztonság területére, tevékenységük összehangolása, további nemzetközi szervezetek munkájába való bekapcsolódás;

- infokommunikációs technológia kockázatkezelési módszereinek fejlesztése és alkalmazása;
- kritikus (információs) infrastruktúrák nyilvánosan hozzáférhető adatainak felülvizsgálata;
- információbiztonsági tudatosság és ismeretek fejlesztése.

Mindehhez igen jelentős kormányzati szintű szabályozási és koordinációs tevékenység, anyagi ráfordítás és számos szakmai szervezet együttműködése szükséges.

Felhasznált irodalom

1. Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the Fight Against Terrorism. Brussels, 20.10.2004 COM(2004) 702 final.
2. Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final.
3. Dr. Haig Zsolt–Dr. Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. 286 p. ISBN: 963-327-391-9
4. Dr. Haig Zsolt: Az információbiztonság komplex értelmezése. Robothadviselés 6. tudományos konferencia kiadványa. Hadmérnök különszám 2006. nov. 22. ISSN 1788-1919. http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/haig_rw6.htm (letöltve: 2008. 02. 15.)
5. Dr. Haig Zsolt: Az információs társadalmat fenyegető információalapú veszélyforrások. Hadtudomány, XVII. évf. 2007. 3. sz. 37-56p. Budapest. ISSN 1215-4121
6. Horváth Pál: Gondolkodjunk el magunkról és a világról. HTE hírlevél 2008. 10. sz. 1-3p.
7. Horváth Pál: Gondolkodjunk el magunkról és a világról. HTE hírlevél 2008. 11. sz. 1-4p.
8. Magyar Információs Társadalom Stratégia. Informatikai és Hírközlési Minisztérium. 2003. november
9. Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. PhD értekezés, 2007.
10. Várhegyi István, Makkay Imre: Információs korszak, információs háború, biztonságkultúra. Budapest, 2000. OMIKK

11. 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. Határozatok tára 31. szám. Budapest, 2008. június 30. 217-231p.