A TÁRSADALOM ÉS A VÉDETT HELYISÉGEK KAPCSOLATA, VALAMINT A VÉDETT HELYISÉGEK KIALAKÍTÁSÁHOZ KAPCSOLÓDÓ TUDOMÁNYTERÜLETEK

RELATIONSHIP BETWEEN SOCIETY AND PROTECTED PLACES AND SCIENTIFIC AREAS RELATED TO THE DESIGN OF PROTECTED PREMISES

BRÉDA GÁBOR PhD-hallgató
Óbudai Egyetem, Biztonságtudományi Doktori Iskola
HAJDU BEÁTA PhD-hallgató
Óbudai Egyetem, Biztonságtudományi Doktori Iskola

Abstract

Our information systems and infrastructures have become indispensable for society. People's lives even if they do not know, in connection with the operation of protected areas will be safe. Maintenance and welfare systems have integrated the elements of information systems, creating a complete infrastructure. Infrastructure planning and operation have become strategically important. Theoretical and physical design of information infrastructures is a complex engineering task, utilizing all technical engineering areas. The built infrastructure also has a protected room that needs to be properly designed and operated. Such a room can serve not only for the protection of technologies, but also for the secure and secure implementation of human-to-human communication. The operation of a well-established infrastructure is fundamentally influenced by the creation of security, so it is in the interest of society to have the right design. The system that is to be set up must also meet the proportional protection requirements in terms of property protection, information security and complex protection of network elements. The topic is comprehensively considered to ensure people's well-being is closely related to the correct design.

1. Bevezetés

A XXI. századi társadalom igényeinek kielégítése érdekében az informatika berendezéseinek valamint azok működtető elemeinek a fejlődése, egy új típusú és rohamos mértékben fejlődő összetett műszaki tudományterület születését idézte elő. Ez a terület az információ-kommunikációs eszközök összekapcsolását és egyre nagyobb hálózatát üzemeltető tudományterület. Az ilyen összekapcsolt és háttéreszközökkel ellátott rendszereket hívjuk összefoglaló néven információs infrastruktúráknak. Más megfogalmazásban az információs infrastruktúra: „A szervezetek vagy szolgáltatások működéséhez szükséges háttér-rendszerek és eszközök állományában megtestesülő fizikai, technológiai és szellemi erőforrások közül mindazok, amelyek a tevékenység végzéséhez elengedhetetlen információkat, illetve azok rendelkezésre állásának és feldolgozásának csatornáit, platformjait és eszközeit biztosítják." (Forrás: internet; Információs infrastruktúra).

2. A megváltozott társadalmi környezet és igényei

Századunk gazdasága információ- és tudásközpontúvá vált, amelyben a gazdasági és társadalmi változásokat az információ-, a számítás- és a távközlési technikák folyamatos megújulása hajtja.

„A XXI. század társadalmi rendje, az információs társadalom a távközlés, a számítástechnika, és az elektronikus média együtteséből létrejövő információs hálózatokra épül.”.[1]

E társadalmat a globalizáció, az új termékek, szolgáltatások kialakulása, új munkastruktúrák megjelenése, valamint a világ bármely részén lévő információforrásokkal való kétoldalú kommunikáció, és ezzel a demokrácia gyakorlásának új eszközei jellemzik.[2] Az új környezet fő jellemzői:

- az információk nagy tömegben történő előállítása, továbbítása és felhasználása,
- a távolság és idő korlátainak leomlása,
- az elektronikus ügyintézés uralkodóvá válása,
- az élet és munkakörülmények megváltozása,
- a kultúra és az oktatás változásai, az élethossziglan tartó tanulás elterjedése.[3]

„A tudás: hatalom” mondta a 456 éve született Sir Francis Bacon angol államférfi, író és filozófus. Milyen igaza volt, de valószínűleg nem is feltételezte, hogy lesz egy olyan időszak/évszázad, melyre csak ebben a kontextusban tudunk gondolni. A XXI. századi ember számára, hogy a megszerzett tudás tényleg hatalom a hatalom pedig „nagy úr”. Tudással rendelkezni ma befolyást jelent, a befolyás érzékelése pedig mindennél fontosabb a biztonságérzethez, hisz ettől érezzük úgy, hogy megéri élni és mindennap tenni egy adott célért. A tudás és az a felett való birtokviszony az élet minden területére igaz. Igaz a magán életre, de igaz a gazdasági és az ipari szegmensekre is. Az a cég, aki a legfrissebb információval/tudással bír, az szerzi meg a versenyelőnyt, ami nélkülözhetetlen a gazdasági stabilitás eléréséhez. A cél érdekében, hogy a legfrissebb információval rendelkezzen valaki, képes sok mindenre, képes az információt a tudást megszerezni, ellopni, annak ellenére, hogy az életünket már a biztonságtudatos viselkedés ernyője alatt éljük. A XXI. századi ember tisztában van azzal, hogy az információt a tudást védeni kell. Az információ védelem a biztonságtudatosság alapja. Hogy mit tehetünk annak érdekében a biztonságtudatos viselkedés mellett, hogy egy szenzitív információ a mi kezünkben maradjon? A cikk további részében kifejtésre kerül egy válasz, egyféle megoldás a kérdésre. Feltárásra kerül annak minden tudományterülettel való korrelációja.

3. Információs infrastruktúrák

Az információs infrastruktúrák egyre fokozottabb mértékű terjedése és létrehozása az információs társadalom növekvő igényeinek a kielégítése céljából történik. A digitális úton hozzáférhető információ azonnali hozzáférése és áramoltatása iránti igény, nélkülözhetetlen eleme lett napjainknak, mind magán, mind szervezeti szinten. Ezért közös és egy irányba mutató törekvés a minél jobb és gyorsabb adatátviteli csatornák kialakítása. Az összekapcsolódó rendszerek egyik fontos alapvető paramétere, az informatikai és gazdasági jellemzőik mellett az üzembiztosságuk. Nem elég tisztán a digitális jellemzők stabil működése szemszögéből kialakítani a háttér infrastruktúrákat. Az információs infrastruktúrák kialakítása a biztonságtudomány komplex szemszögéből is megfelelőnek kell, hogy legyen. A rendszerelemek működőképessége rendszerint, mindig valamilyen felhasználói

érdekcsoport beruházási és fenntartási igényét kell, hogy teljesítse. A működőképesség megbénulása jelentős szolgáltatásbeli kieséssel valamint kárral járhat, nem csak a létesítő és fenntartó számára, hanem a felhasználó csoportok számára is. Ha közszolgáltatói infrastruktúráról van szó, akkor a társadalom szempontjából is fontos az információs infrastruktúra működése. A fontosságuk rangsorolásával és a kiesésük miatt okozott kár mértéke szempontjából valamint a betöltött funkcióik szerint az ilyen infrastruktúrákat és ezzel együtt az ilyen infrastruktúra információs rendszereit kritikus infrastruktúra megjelöléssel láthatjuk el. Európai Uniós jogalkotás szintjén 2016. július 6-án megjelent „Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve", amely NIS irányelv elnevezéssel is ismert. A megjelent irányelv II. melléklete tartalmazza azoknak az alapvető szolgáltatásokat nyújtó szereplőknek a listáját, akik ilyen csoportba tartoznak. Ilyenek megjelölésűek azok:

- amely szervezetek a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújtanak,
- akiknek az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ; és
- az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában (Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve).

Az információs infrastruktúrák méretük szerint lehetnek világméretű (globális), regionális (kontinens méretű) vagy nemzeti (országos méretű) kiterjedésűek. A tárgyalt infrastruktúrák kialakításuk és a létesítésük szempontjából a gyakorlati szempontokat figyelembe véve többféle megközelítés és lehetőség alapján kerülhetnek kialakításra. Szempont lehet a földrajzi elhelyezés pl.:ásványkincs, energiahordozó előállási helye, de lehet centralizált megvalósítás is mint például információs központok, energia átalakító létesítmények, valamint szempont lehet kimondottan a stratégiai biztonság megvalósítása is.[4]

4. Kapcsolódó tudományterületek

A témában szóban forgó létesítmények megvalósítása tekintetében, számos tudományterület és szakma képviselteti magát. Áttekintve az együttműködő műszaki területeket, első megközelítésben a következő tudományágak szakértelmét kell igénybe venni egy kialakítandó objektum megteremtése érdekében:

- informatika,
- villamos távközlés,
- biztonságtudomány,
- geológiai ismeretek és tudományok területe,
- meteorológiai ismeretek,
- hadászat, hadbiztonság,
- építészet,
- villamos energetika,
- gépészet, gépész energetika területe.

Egy infrastruktúra elképzelése és tervezése során az informatikai rendszer és a védelem kialakítása a létesítmény tervezése idején együtt járó párhuzamos feladatok. Megközelíthetjük a témát úgy is, hogy egy olyan objektumot kell kialakítani ahol az információs infrastruktúrák rendszerelemei különböző szempontok szerint kialakított védett helyiségekbe kerülnek, és azok valamilyen informatikai adatátviteli csatorna révén egymással kommunikálni tudnak.

5. Információs infrastruktúrák kialakítása

Információs infrastruktúra kialakítása több különböző kiinduló állapotból lehetséges.

Az első, hogy a kialakítani kívánt infrastruktúra még nem létezi. Új tervek alapján új helyszínen, majdani új épületben, még nem épített környezetben kívánják kialakítani azt.

A következő állapot, amikor az épület és helyszín adott, de még nincs semmilyen informatikai infrastruktúra kialakítva. Kész épület falai közé kell kialakítani a kívánt infrastruktúrát.

És a harmadik állapot amikor a helyszín és a környezet adott. Van valamilyen információs infrastruktúra, és annak a bővítése, felújítása vagy a létező mellé egy új rendszer kiépítése a feladat.

A tervezői szempontból a legnagyobb, és a legszebb állapot a semmiből való építkezést. Először ki kell jelölni egy helyet a leendő infrastruktúra helyszínéül. Végig kell gondolni a helyszíni adottságokat amelyek a kialakítandó infrastruktúrát fogják érni. Ez a fent felsorolt mérnöki tudományok több területét is igényli. Érdemes jól megközelíthető több irányból is elérhető helyet választani egy leendő kialakítás számára oly módon, hogy az mesterséges akadályokkal elzárható legyen, azonban igény esetén azonnali hozzáférést biztosítson. Érdemes olyan helyszínt keresni, amely katonailag is jól védhető, illetve egyébként is védett helyszín közelében van. A létesítés helyszínén előforduló természeti jelenségeket is meg kell vizsgálni, mivel azok előfordulása nagymértékben befolyásolhatja a leendő infrastruktúránk működésének stabilitását. Fontos körültekintőnek lenni, mivel egy ilyen új infrastruktúra kialakítása, akár több évtizedes működést is kell, hogy átíveljen. A következő szempont lehet az energiaigény. A költségek szempontjából, érdemes megvizsgálni a már kiépített energiatovábbító infrastruktúrákat is a megvalósítás helyszínén. Ellátásbiztonság szempontjából, egy új tápláló vezeték akár villamos, akár gázvezetékről lévén szó, jelentős beruházási költségeket jelent egy építkezés kivitelezése során. A legjobb lehetőség olyan helyszín kiválasztása az egyéb szempontokat szem előtt tartva ahol több független megtáplálási útvonalat is ki tudunk alakítani a közelben lévő üzemelő megtáplálási helyekről. A nagyvárosok környezete ezért is előnyös lehet, mivel alapjába véve az ilyen helyek az ellátásbiztonság szempontjából jónak tekinthetőek. Amennyiben a második és harmadik kialakítási esetet vesszük figyelembe, egy meglévő objektumban kell információs infrastruktúrát kiépíteni, ott meg kell vizsgálni a kiépített energetikai infrastruktúrák jelenlétét. Ki kell alakítani a kívánt folyamatos működést biztosító igényeknek megfelelően. Meg kell vizsgálni a több utas energia betáplálások lehetőségét, a gáz szolgáltatás megfelelőségét, valamint az áthidaló backup energiaforrások elhelyezhetőségét. A fizikai létesítés helyének kialakítása során szem előtt kell tartani a statikai megfelelőség mellett a fizikai biztonság kritériumainak a teljesíthetőségét is. Itt a falazat anyaga, vastagsága, valamint a megközelítés, bejutás lehetősége, a megfelelő kialakíthatóság szempontjait már a korai szakaszban a tervekben kell, hogy meghatározzák. Állami környezetben, a minősített adatok tárolását illetően találunk előírást a védelem kialakítására. Ez konkrét fizikai védelmi előírás, amely a 90/2010 (III. 26.) Kormányrendelet „V. Fizikai biztonság” fejezetében található.

A védelmi megoldások kialakítása során előfordulhat különböző speciális műszaki védelmi megoldások igénye. Két ilyen példát említve igény lehet az elektromágneses árnyékolás kialakítása, vagy különálló fizikailag elválasztott hálózatok egymás melletti üzeme. Az első példát szemügyre véve, elterjedt nézet, hogy az információs infrastruktúrák eszközeinek elektromágneses kisugárzása, információtartalommal bír. Védeni kívánt adatközpontok esetén, ki kell zárni minden olyan elvi biztonsági rést, amely szivárgási csatornaként jelentkezhet. Másfelől a példánál maradva a természeti jelenségek kíséretében keletkező, valamint esetleges hadi tevékenységek során létrehozott nagy energiájú elektro-

mágneses impulzusoktól is védeni kell az arra érzékeny készülékek sértetlenségét. Így a mágneses árnyékolás megvalósításával kétirányú védelmet valósíthatunk meg.[5]

A második példa igénye olyan helyszínen jelentkezhet, ahol a helyi munkaállomások kialakítása során az informatikai biztonság követelménye lehet több informatikai rendszer autonóm módon történő együttes alkalmazására. A rendszerek lehetnek szigetüzeműek, a világháló felé nyitottak, vagy a kettőt egymás mellett külön kialakítva. Itt a különböző kialakítási formák miatt, nehézségekbe ütközhet a tervezés és a kivitelezés. A két hálózatot egymás mellett megalkotva, sokszor az építőelemeket duplikálva olyan megoldásokat kell kialakítani, amelyek informatikailag függetlenül biztosítják a két rendszer egyidejű, egymás melletti működését. Az információs infrastruktúrák fizikai védelemét, a speciális igényeket leszámítva, az objektumvédelem bevált elvei alapján a szokásos védelmi eszközökkel kell kialakítani. Héj védelmi modellt alkotva, az egyenszilárdságra törekedve kell kialakítani azt. Visszakanyarodva az információs infrastruktúra létrehozása során szükséges műszaki tudományágakhoz, a biztonságtudomány és az építész tudomány területe jelentkezik újból. Az építész szakágat megfelelő információkkal kell ellátni a fizikai védelemnek megfelelő anyagokkal való tervezéséhez. További biztonsági követelmény az infrastruktúra épségének védelme az elemi erőkkel szemben. Tűzjelző rendszert kell kialakítani a helyiségek tekintetében, figyelemmel a kábelalagutak és az álmennyezettel takart részekre. Speciális igény lehet a nagy értékű berendezések esetén automatikus tűzoltó berendezés, föld alatti elhelyezés esetén víz jelző berendezés kialakítása is. A fizikai védelem kialakítása során az elektronikus jelzőeszközök használata célszerű. Belülről kifelé haladva, a belső terekben fizikai jelenlét, üvegtörés és a nyílászárókra nyitásérzékelőket kell elhelyezni megfelelően tagolva, zónákra és külön részekre osztva ezzel a védeni kívánt tereket. Fontos a különböző védett részek beléptető rendszerrel való kialakítása is, a jogosultak pontos meghatározása mellett. Az átlépések naplózott formában kell, regisztrálva legyenek. Az eddig elképzelt elektronikus vagyonvédelmi rendszerrel, a külső hatásoknak ellenálló információs infrastruktúrának helyet adó objektumot a védelem fokozása érdekében célszerű élőerős őrzés védelmi funkció kialakításával megvalósítani. Az őrszolgálat feladata igen sokrétű. Végzik az objektumba történő be és ki léptetést, a lezárt zónák eseményit figyelik, és incidens esetén intézkednek az infrastruktúra védelmének fenntartásával. Az objektumvédelem korszerű eleme a videó megfigyelő rendszer. Segítségével az őrszolgálat jelentős számú terület egyidejű vizuális ellenőrzését végezheti. Ez mellett további előny az események rögzíthetősége is, amely későbbi vizsgálat esetén hasznosnak bizonyulhat. Az infrastruktúra fizikai védelmének további eleme a különböző telekhatárokon elhelyezkedő árok, sánc, kerítés kialakítása. Ez az elem a külső védelmi kör, amely pontosan kijelöli azt a határt, ami bárki által még megközelíthető és meghatározza a védelem szempontjából azt a vonalat, ahonnan intézkedni szükséges egy engedély nélküli telekhatár átlépés esetén.[6]

5.1. Az átviteli út

Az információs infrastruktúrák elkerülhetetlen és nélkülözhetetlen eleme az információs hálózatok további információs hálózataival összekötő átviteli út és annak védelme. Az információs összeköttetés fizikai szintje három fizikai jelenségre, és annak hírközlési technológiáira osztható. Az első a vezetés, a vezetékes összeköttetés, amely réz vezető érpárokon keresztül biztosítja az informatikai berendezések távoli összeköttetését. A második megoldás szintén kábelszerű megoldás de itt az átvitel a fény segítségével történik, ez nem más mint az optikai kábel. A harmadik csoport a vezeték nélküli távközlés, amely rádiós hullámok útján köti össze a kommunikáló informatikai berendezéseket. A legnagyobb átviteli sebességet és a legstabilabb üzemet manapság,

az optikai kábeleken keresztül érhetjük el. Ez a technológia folyamatosan szorítja ki a hagyományosnak mondható vetélytársait, azonban a teljes térnyerés a helyi, kis kiterjedésű lokális összeköttetések megvalósítási technológiái miatt még várat magára. A vezeték nélküli kis távolságú helyi, valamint a mobil adat alapú távközlés szintén dinamikus ütemben fejlődik, egyre biztonságosabb és gyorsabb protokollok kidolgozása kerül bevezetésre, azonban a nagy információs rendszerek további rendszerekkel való összeköttetése napjainkban csak stabil megoldások révén képzelhető el. A kábelszerű információs adatátviteli utakat üzembiztonságát természetesnek vesszük de azok szakadása jelentős kiesést generálhat az információáramlás és az ellátás folyamatában. A vezetékes átviteli utak üzembiztosságát réz érpárok esetén, időszakos vezeték paraméter mérésekkel, folytonossági hiba esetén FDR (frequency domain reflectometry) méréssel vizsgálhatjuk. Optikai szál esetén OTDR (optical time domain reflectometer) berendezésekkel biztosíthatjuk egy szakasz folyamatos felügyeletét. Az OTDR felügyelet a soros hiba azonnali kimutatása mellett a lassan előálló soros vonali hiba kialakulásának előrejelzésére is használható, mivel kialakításának és alapelvének köszönhetően folyamatosan figyeli a monitorozott optikai szál fizikai paramétereit az üzem fenntartása közben.[7]

A rádiós zártláncú mikrohullámú összeköttetések, szintén több évtizedes múltra tekintenek vissza. Az átviteli hiba lehetőségei itt a végponti berendezésekre, egymás láthatóságának akadályoztatására illetve rádiós zavartatásra vezethetőek vissza.

Az átviteli utakon haladó jelek információvédelméről, legyen az bármely a felsoroltak közül, szintén gondoskodni szükséges. A megoldást a kriptográfia eszközei közt kell keresni, amelyre megoldás a kódolás, rejtjelezés és titkosítás alkalmazása.

5. Összegzés

Jelen cikkben egyfajta áttekintést kaphatunk az információs infrastruktúrákról, azoknak a társadalom számára elfoglalt helyéről, a megvalósítás során kapcsolódó műszaki területektől és a kapcsolódó biztonság szerteágazó volumenéről. Az ilyen infrastruktúrák kialakítása, komplex mérnöki feladat, mivel az informatikai működőképességen kívül számos kritériumnak meg kell, hogy feleljenek. Stabilnak kell lenniük és a külső hatásokkal szemben védettnek. A védelem kialakítása során az objektumvédelem megfelelő kialakítása mellett láthatjuk, hogy az információs rendszerek egyes elemeinek, lokális helyeken egyedi védelmi igényei is felmerülhetnek. Ezeket a védett helyiségeket egyedi védelmi megoldásokkal alakíthatják ki, a külső és belső hatásokkal szemben. A kiterjedt információs rendszereknek alapvető tulajdonsága lehet, hogy más fizikai helyen lévő rendszerek számára is elérhetőek kell legyenek, különböző adatátviteli csatornákat használva. Ezeket a csatornákat, mint potenciális hibaforrásokat és lehetséges információszivárgási réseket szintén védelmi megoldásokkal kell ellátni a védelmi elemek arányos alkalmazásával.

Jegyzetek

1. Blahó András (2002): Európai integrációs alapismeretek, Aula Kiadó, Budapest, 540. o.
2. Illés Sándor (2003): Úton az információs társadalom felé, IV. Nemzetközi (Jubileumi) Konferencia, Miskolci Egyetem, Gazdaságtudományi Kar, Miskolc-Lillafüred, 2003. május 26–27.
3. Blahó András (2002): i. m.
4. Rajnai Zoltán, Fregan Beatrix; Kritikus infrastruktúrák védelme, XXI. Fiatal Műszakiak Tudományos Ülésszaka, 2016. Kolozsvár, 349–352. http://eda.eme.ro/bitstream/handle/10598/29102/EME_21_FMTU_2016_RajnaiZoltan-FreganBeatrix.pdf?sequence=3 (letöltve: 2017. 01. 05.); Varga Péter János (2008): A kritikus információs infrastruktúrák értelmezése; Hadmérnök, III. évfolyam 2. szám. 2008. június.; Haig Zsolt, Kovács László (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák; Tanulmány. http://uni-nke.hu/downloads/konyvtar/kovasz/kritikus_infrastrukturak.pdf (letöltve: 2017. 01. 05.)
5. Ványa László mk. alezredes; Zrínyi Miklós Nemzetvédelmi Egyetem (2001): Az elektronikai hadviselés eszközeinek,rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre, Doktori (PhD) értekezés 2001. http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2003/vanya_laszlo.pdf (letöltve: 2017. 01. 06.); Szűcs Péter (2002): Műholdas személyi kommunikációs rendszerek állóképessége a rádiófrekvenciás-, nagyfrekvenciás- és elektromágneses impulzus fegyverek ellen; Repülőtiszti Intézet Repüléstudományi közlemények, ZMNE. http://nbsz.gov.hu/docs/pub_muholdas_szemelyi_allokepesseg.pdf (letöltve: 2017. 01. 06.); Szűcs Péter (2014): Műholdas kommunikációs rendszerek támadhatósága 2014. http://epa.oszk.hu/02500/02538/00002/pdf/EPA02538_nemzetbiztonsagi_szemle_2014_01_159-169.pdf (letöltve: 2017. 01. 06.)
6. Berek Lajos (2014): Biztonságtechnika, NKE, Budapest, 2014. http://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf (letöltve: 2017. 01. 06.); Berek Lajos, Berek Tamás, Berek László (2016): Személy és vagyonbiztonság, ÓE, Budapest, 2016. ISBN 978-615-5460-94-4 http://asp01.ex-lh.hu:80/R/-?func=dbin-jump-full&object_id=23873&silo_library=GEN01 (letöltve: 2017. 01. 06.)
7. Bréda Gábor: (2014): Optikai szálfelügyeleti rendszer tervezése, Diplomamunka, Óbudai Egyetem, Budapest.

Felhasznált irodalom

90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1000090.kor (letöltve: 2017. 01. 06.)

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, II. számú melléket. http://eur-lex.europa.eu/legalcontent/HU/TXT/PDF/?uri=CELEX:32016L1148&from=HU (letöltve: 2017. 01. 05.)

Berek Lajos, Berek Tamás, Berek László (2016): Személy és vagyonbiztonság, ÓE, Budapest, 2016. ISBN 978-615-5460-94-4 http://asp01.ex-lh.hu:80/R/-?func=dbin-jump-full&object_id=23873&silo_library=GEN01 (letöltve: 2017. 01. 06.)

Berek Lajos (2014): Biztonságtechnika, NKE, Budapest, 2014. http://real.mtak.hu/19709/1/biztonsagtechnika.original.pdf (letöltve: 2017. 01. 06.)

Blahó András (2002): Európai integrációs alapismeretek, Aula Kiadó, Budapest, 540. o.

Bréda Gábor: (2014): Optikai szálfelügyeleti rendszer tervezése, Diplomamunka, Óbudai Egyetem, Bp.

Haig Zsolt, Kovács László (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák; Tanulmány. http://uni-nke.hu/downloads/konyvtar/kovasz/kritikus_infrastrukturak.pdf (letöltve: 2017. 01. 05.)

Illés Sándor (2003): Úton az információs társadalom felé, IV. Nemzetközi (Jubileumi) Konferencia, Miskolci Egyetem, Gazdaságtudományi Kar, Miskolc-Lillafüred, 2003. május 26–27.

Információs infrastruktúra: http://www.bgalapitvany.hu/2016/05/informacios-infrastruktura-information-infrastructure/ (letöltve: 2017. 10. 05.)
Rajnai Zoltán, Fregan Beatrix (2016): Kritikus infrastruktúrák védelme, XXI. Fiatal Műszakiak Tudományos Ülésszaka, 2016. Kolozsvár, 349–352. http://eda.eme.ro/bitstream/handle/10598/29102/EME_21_FMTU_2016_RajnaiZoltan-FreganBeatrix.pdf?sequence=3 (letöltve: 2017. 01. 05.)
Szűcs Péter (2014): Műholdas kommunikációs rendszerek támadhatósága 2014. http://epa.oszk.hu/02500/02538/00002/pdf/EPA02538_nemzetbiztonsagi_szemle_2014_01_159-169.pdf (letöltve: 2017. 01. 06.)
Szűcs Péter (2002): Műholdas személyi kommunikációs rendszerek állóképessége a rádiófrekvenciás-, nagyfrekvenciás- és elektromágneses impulzus fegyverek ellen; Repülőtiszti Intézet Repüléstudományi közlemények, ZMNE. http://nbsz.gov.hu/docs/pub_muholdas_szemelyi_allokepesseg.pdf (letöltve: 2017. 01. 06.)
Ványa László mk. alezredes; Zrínyi Miklós Nemzetvédelmi Egyetem (2001): Az elektronikai hadviselés eszközeinek,rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre, Doktori (PhD) értekezés 2001. http://uninke.hu/downloads/konyvtar/digitgy/phd/2003/vanya_laszlo.pdf (letöltve: 2017. 01. 06.)
Varga Péter János (2008): A kritikus információs infrastruktúrák értelmezése; Hadmérnök, III. évfolyam 2. szám. 2008. június.