Óbudai Egyetem
Doktori (PhD) értekezés

A kritikus információs infrastruktúrák biztonságos üzemeltetésének vizsgálata hálózatelméleti megközelítésből, az ember-technika-környezet relációjában

Puskás Béla

Témavezető:

Dr. Magyar Sándor

Biztonságtudományi Doktori Iskola

Budapest, 2017

Szigorlati Bizottság:

Elnök:

Prof. Dr. Berek Lajos, egyetemi tanár, ÓE

Tagok:

Dr. habil. Farkas Tibor, egyetemi docens, külső NKE

Dr. habil. Kerti András, egyetemi docens, külső NKE

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Berek Lajos, egyetemi tanár, ÓE

Titkár:

Dr. Kiss Gábor, egyetemi docens, ÓE

Tagok:

Dr. Bérczi László tű. dandártábornok, külső

Dr. habil. Farkas Tibor, egyetemi docens, külső NKE

Dr. habil. Michelberger Pál egyetemi docens, ÓE

Bírálók:

Dr. Krasznay Csaba adjunktus, külső NKE

Dr. Horváth Zsolt László adjunktus, ÓE

Nyilvános védés időpontja

2017.10.11.

TARTALOMJEGYZÉK

BEVEZETÉS

„The whole is more than the sum of its parts.”

„Az egész több mint a részek összege.”

Arisztotelész

A kritikus informatikai rendszerek biztonságos üzemeltetése több összetevőből áll. Ahhoz, hogy egy rendszer az életciklusa egészében biztonságosan működjön elengedhetetlen az üzemeltetésbiztonság magas színvonalú biztosítása. A kutatásom során ezt a területet vizsgáltam meg részletesen.

Az értekezésemben bemutatom, hogy egy adatközpont milyen bonyolult felépítésű, mennyi mindennel kell számolni, és milyen összetett komplex rendszert alkot az elemek sokasága. A rendszerelemek közül részletesebben tárgyalom az adatközpont felépítését és kevésbé részletesen a hardvereket, a szoftvereket és a technológiákat. Említést teszek még olyan összetevőkről, mint a pénzügyi, a humán erőforrás, vagy éppen a szabályzók, amelyek szintén fontos építőelemei az infrastruktúrának.

Két fizikai IT hálózat között megjelenik az ember, a társadalmi hálózat, ami virtuális kapcsolatot teremt a két hálózat között. Az értekezésben választ keresek arra a kérdésre, hogy az ember kapcsolata a rendszerrel hogyan befolyásolja annak működését.

A kutatásom során tanulmányoztam számos kritikus informatikai rendszer fizikai és logikai hálózatait, melyeket a banki, az ipari, a katonai szférában használnak. Az így feltárt adatokból hipotézist állítottam fel, hogy milyen változtatások szükségesek a szabályzókban.

Az értekezés terjedelmi korlátja és a feldolgozandó téma széles spektruma miatt nem volt célom a hálózatelmélet és az információbiztonság önálló tárgyalása. A hálózatelmélet rövid ismertetése azt a célt szolgálja, hogy az alapok bemutatásával rávilágítsak arra, hogy a rendszerszemléletű gondolkodás hogyan segítheti a kritikus informatikai rendszerek biztonságosabb üzemeltetését.

Biztonság alatt az üzemeltetés biztonságot értem, amely nem feltétlenül jelenti az informatikai biztonságot és főleg nem az információbiztonságot. Az értekezésem egyik célja, hogy üzemeltetési oldalról világítsak rá a kritikus informatikai rendszerek biztonságos üzemeltetésére, amely ebből a megközelítésből az üzemeltetésbiztonságot jelenti. A biztonság komplexitása miatt több esetben érintem az információbiztonságot

és az informatikai biztonságot is, de részletesen csak az üzemeltetésbiztonságot tárgyalom.

A kutatásom és a munkám során megszerzett minősített anyagokat [1] nem dolgoztam be az értekezésembe. Az értekezésem tudományos jelentőségét arra alapoztam, hogy az informatikai üzemeltetésnek komplex hálózatelméletű alapokkal megerősített gondolkodásmód feldolgozásával a terület új értelmezést nyer. A kutatásom megkezdése előtt tapasztalataim szerint csak részterületek voltak feldolgozva, kidolgozva egymástól függetlenül. Természetesen többen foglalkoztak már hálózatkutatással, helyi szinten vannak informatikai üzemeltetés szabályozások, továbbá számos szervezet megfelelően tárolja a konfigurációs adatokat, de egyben az egész nincs jelen.

A tudományos probléma megfogalmazása

A kritikus informatikai rendszerek – mint az élet számos területén megtalálható egyéb más rendszerek is – bonyolult hálózati felépítést mutatnak. Hálózat alatt nem csak az IT [2] hálózatot értem. A társadalmi-, közösségi-, közlekedési-, szövetségi-, jogszabályi stb. hálózatokat és ezek IT rendszerhez kapcsolódó pontjait, „átjárókat" is elemezni kell. A biztonságos üzemeltetéshez ismerni kell az elemeket, amelyekből felépül a rendszer, továbbá az egymásra gyakorolt hatásokat, hatásmechanizmusokat is. El kell készíteni a fizikai és a logikai térképeket, amelyek véleményem szerint nem csak a hagyományos értelembe vett komponenseket tartalmazzák (router [3], kliens [4], kiszolgáló [5] stb.), hanem a környezetet is. Természetesen vannak kritikus elemek és lehetnek olyan alkotórészek, amelyek kiesése nem jelent problémát a rendszer egészére. Az informatikai rendszert nem önmagáért üzemeltetjük, hanem egy cél érdekében. A kritikus informatikai rendszerek létfontosságú infrastruktúrát szolgálnak ki ezért is tartottam fontosnak azok részletesebb tanulmányozását.

[1] Minősített anyag alatt olyan adatokat értek, amelyet a minősített adat védelméről szóló 2009. évi CLV törvény 3. § határoz meg.
[2] IT (Information Technology) Információ-Technológia
[3] Magyar fordítása útválasztó, egy olyan eszköz, amelyet a számítógépes hálózatokban használnak. A szakmában főleg, de a közéletben is az angol eredeti szó terjedt el, így az értekezésemben is a router szót használom a továbbiakban is.
[4] Ebben a kontextusban a számítógépes hálózatban lévő végfelhasználó eszközt értem.
[5] A számítógépes hálózatokban a szervereket sorolják ide.

Kovács László hivatkozva az európai programról szóló Zöld Könyvre[6] az írja, hogy a „*kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, internet, műholdak stb.)*” [1]

Az üzemeltetésben a számos környezeti hatás mellett a legmeghatározóbb talán az ember és az őt, az ő kapcsolatát a rendszerrel szabályzó jogszabályi háttér. Az informatikai üzemeltetés során felhalmozott személyes tapasztalatom, a konferenciákon való részvételeim, a szakirodalomban leírtak, valamint a szakmában dolgozókkal folytatott személyes megbeszélések során azt tapasztaltam, hogy hiányosságok mutatkoznak ezen a területen. Az információbiztonság területén hatalmas lépések történtek kormányzati szinten, azonban a kritikus informatikai rendszerek üzemeltetésével csak az informatikai biztonság kapcsán foglalkoznak a szabályzók. Az informatikai vezetők magukra vannak hagyva döntéseikben, a képzésekben, sokszor személyes képességeiken múlik, hogy meggyőzzék a vezetést egy-egy döntés fontosságáról. A másik problémát a rendszerszintű, átfogó gondolkodás hiányosságában látom. Ebben segítene a hálózatelméletű megközelítés. Ehhez a gondolatmenethez szorosan kapcsolódik a rendszerelemek pontos nyilvántartása, valamint az ezekhez kapcsolódó folyamatok pontos definiálása, amelyek sok esetben az állami szektorban hiányosak. Az értekezésben rámutatok, hogy amennyiben rendszerszemléletben gondolkodunk és a hálózatelméleti kutatások eredményeit is helyesen tudjuk alkalmazni, akkor lehetőség nyílik egy olyan szoftver megalkotására, amely segíteni tudja a magas rendelkezésreállást a kritikus információs infrastruktúrákban. Ezzel növelhető az informatikai rendszer biztonságos működése is.

Célkitűzések

A doktori értekezés célja, hogy rávilágítsak a rendszerszemlélet fontosságára és a kritikus információs infrastruktúra üzemeltetésében feltárjak olyan hiányosságokat, amelyek kiküszöbölésével az üzemeltetés biztonsága jelentősen javítható Magyarországon.

[6] Zöld Könyv alapja volt a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvénynek.

A doktori értekezésben az alábbi célokat határoztam meg:

1) A szakirodalom feldolgozását követően bemutatom a hálózatelméleti alapokat, amelyek szoros kapcsolatban állnak a rendszerszemléletű gondolkodással és a rendszermodellezéssel egyaránt.

2) Célom felkutatni, hogy milyen összefüggés lehetséges az ember és az általa üzemeltetett informatikai rendszer között, illetve milyen környezeti tényezők befolyásolják az informatikai rendszerek működését.

3) Célként fogalmaztam meg, hogy megvizsgáljam, milyen struktúrát kell megkövetelni a szervezeti felépítésben, az infrastruktúrában vagy a jogi környezetben.

4) Felkutatom a kritikus informatikai rendszerek, a kapcsolódó kritikus infrastruktúrák üzemeltetésével, védelmével kapcsolatos jogszabályokat. A jogszabályi hiányosságok feltárását követően megfogalmazom, milyen keretek között kell üzemeltetni a kritikus informatikai rendszereket és milyen területeknél szükséges új jogszabály kidolgozása.

5) Az előző célokban megfogalmazott információk birtokában célom meghatározni egy informatikai rendszer üzemeltetését támogató szoftver alapkritériumait.

A téma kutatásának hipotézisei

H1: Feltételezem, hogy a többdimenziós hálózatelméleti alapok alkalmazásának bevezetése elősegíti a számítógépes adatfeldolgozással a biztonságosabb és komplexebb informatikai rendszerüzemeltetést.

H2: A sikeres informatikai üzemeltetés érdekében feltételezhető, hogy egy szigorúan szabályzott struktúrát kell kiépíteni, a szervezeti felépítésben, a környezeti jogszabályok területén és az informatikai rendszert kiszolgáló infrastruktúrában.

H3: Feltételezem, hogy jelenleg Magyarországon az állami szektorban lévő kritikus informatikai rendszerek üzemeltetéséhez szükséges – a biztonsági aspektust leszámítva – jogszabályi hátterek hiányosak.

H4: Hipotézisem szerint szükséges egy specializált, kibővített Konfigurációt Kezelő Rendszer[7] kialakítása, bevezetése és folyamatos továbbfejlesztése a kritikus informatikai rendszerek biztonságos és megbízható üzemeltetése érdekében.

[7] CMS (Configuration Management System) Konfigurációt Kezelő Rendszer

A téma kutatásának módszerei

Kutatásom során egyaránt alkalmaztam az empirikus (tapasztalati) és az elméleti kutatási módszereket.

Az elméleti kutatásomban nagy szerepe volt a szintézisnek, ahol az egyes elemeket viszonyítottam az egészhez és a közöttük lévő kapcsolatrendszert térképeztem fel.

Induktív módszerekkel feldolgoztam az évek alatt összegyűlt tapasztalataimat, amelyekből általánosításokat tettem. Ezután az általánosításokat megvizsgálva meggyőződtem azok helyességéről. Az ellenkező irányú módszer alkalmazásakor (deduktív) megvizsgáltam, hogy az általánosságban megfogalmazott állítások a valóságban hogyan érvényesülnek a konkrét területeken, egyedi esetekben.

A feladatom elvégzéséhez a személyes konzultációk során, a kutatási cél elérése érdekében a következő területekkel ismerkedtem meg:

Felkerestem a kutatási témában eredményeket elért kutatókat, szakembereket, cégeket, szervezeteket. Helyszíni bejárás során tanulmányoztam több Magyarországon működő cég kritikus infrastruktúrájának felépítését, valamint irányításának, felügyeletének és üzemeltetésének kialakítását. Szakirodalmak, szakértők segítségével tanulmányoztam a mai kor színvonalának megfelelő kiemelten védett adatközpont kiépítésének követelményeit. Személyes tapasztalatot szerezhettem egy kiemelten védett Magyarországi adatközpont megtervezésében és kivitelezésének irányításában, valamint tanulmányoztam a NATO új főhadiszállásának adatközpont kiépítését, részt vettem az adatok migrálásának megtervezésében.

A kutatás során összegyűjtött információkat rendszereztem, az azokból felvetődött kérdésekre válaszokat kerestem.

1. FOGALMI MEGHATÁROZÁSOK

Az informatikai rendszert az ahhoz kapcsolódó folyamatok és az üzemeltetés során egy-egy pillanatban megfigyelhető állapot, állapotváltozások hálózati struktúrája alkotja.

Mint minden tudományos kutatásban fontos tisztázni a fogalmakat, annak érdekében, hogy a definíciókban leírtak egyértelműen meghatározzák az egyes területeket, elemeket. A fejezetben tisztázom az alapfogalmakat úgy, mint mi a rendszer, mit nevezünk komplex rendszernek, mi a hálózat, mi az informatikában a biztonság, mi a kritikus infrastruktúra és mi a kritikus információs infrastruktúra meghatározása.

1.1. HÁLÓZAT

„Az Internet az első dolog, amit az ember épített, s amit mégsem ért. Ez a valaha volt legnagyobb kísérlet az anarchiára.”

Forrás: [2][8]

Az Amerikai Védelmi Minisztérium a magas színvonalú haditechnikai fejlesztések érdekében 1958-ban létrehozatta az ARPA-t[9]. Paul Baran[10] 1964-ben kifejtette: ahhoz, hogy létrehozzunk egy olyan kommunikációs csatornát, amely egy támadás okozta sérülékenységet minimalizálja, az eddigi centralizált hálózatok helyett elosztott hálózatot kell létrehozni. Úgy gondolta, hogy az így kialakított interneten adatcsomagokat kell továbbítani, melyek egymástól függetlenül érhetnek akár más-más csomópontokon keresztül a célállomásig. Akkor az ötletét elvetették, de később 1969-ben létrehoztak egy kísérleti hálózatot, amelyhez később már többen csatlakoztak. [3] [4] [5]

1970-es években az internet elkezdte élni saját életét, amely már túlmutatott azokon a terveken, amelyet annak idején megálmodtak. Egyre több intézmény csatlakozott a hálózathoz, azonban nem Baran elgondolása szerint történtek a dolgok. Nem egy elosztott hálózat jött létre, hanem egy skálafüggetlen modell kezdett

[8] Az értekezésben az oldalszám megjelölés nélküli forrásmegjelölésre akkor kerül sor, ha az egy weblapról származik.
[9] ARPA (Advanced Research Projects Agency) Fejlett Kutatási Projektek Ügynöksége
[10] Paul Baran (1926-2011) lengyel születésű, amerikai mérnök.

kialakulni. A rendszert – gyors fejlődése és a kiterjedése miatt – nem lehetett már egy kézben tartani. Már nem az eredeti cél volt a meghatározó, hogy egy támadás esetén is egy működőképes hálózat biztosítsa a kommunikációt. Ezzel szemben létrejött a ma ismert internet, amely a véletlen hibákkal szemben rendkívül ellenálló. Az internet egy komplex rendszerré nőtte ki magát. [6]

Az internet létrejöttekor hasonló hálózat alakult ki, mint amivel az élet számos területén találkozunk. Ilyenek például a társadalmi hálók, az emberi testben fellelhető bonyolult hálózatok (idegrendszer, sejtekben lévő kapcsolatok stb.), de ilyenek a járványok terjedését leíró modell mellett még sok egyéb más hálózat is. Ahhoz, hogy megérthessük a hálózatok működését fontos a rendszer elemeinek pontos meghatározása, a közöttük lévő kölcsönhatások és összeköttetések feltárása és a hálózati térkép, topológia ismerete. [7]

Az értekezésben a kritikus információs infrastruktúrák biztonságos üzemeltetését hálózatelméleti megközelítésből vizsgálom, ezért fontosnak tartom a hálózat fogalmának meghatározását.

A kutatásom során megkíséreltem felkutatni a témával foglalkozó tudományos publikációkat. Ekkor találtam rá Munk Sándor 2010-ben megjelent publikációjára, melynek a címe *Hálózatok fogalma, alapjai*. A cikk célja az volt, hogy választ adjon mit is nevezünk hálózatnak és bemutatta azok különböző alkalmazási típusait. Érdekes, hogy látszólag mást jelentett a hálózat kifejezés régebben és mást jelent ma. Ahogyan változott a környezet, úgy változott a fogalom is. Ma is mást értenek a hálózat fogalma alatt a társadalomtudományban, a távközlésben, az IT világban, villamos energia szolgáltatóknál, a kommunikációban, a biológiában, a szociológiában és az élet számos területén. Azonban nehezen található egy egységes meghatározás arra, hogy mi is a hálózat. A tanulmány megállapítása szerint a hálózat összekapcsolt elemek, objektumok rendszere. Munk Sándor a tanulmányában megemlíti egy számomra fontos típusát a hálózatnak, ez pedig az információkat továbbító, elosztó hálózatok. [8]

Munk Sándor által publikált cikkben megtalálható a hálózat definíciója, miszerint:

„A hálózat a hálózattudomány fogalomrendszerében a valóságban létező fizikai, biológiai és társadalmi objektumok absztrakciója, vagyis a hálózat mindig a megfigyelhető valóság egy reprezentációja, vagy modellje és nem a valóság maga”

Forrás: [8] 182. o.

Haig Zsolt és Kovács László tanulmányában olvasható mondatok összecsengenek a dolgozatom első fejezetében leírt Eric Emerson Schmidt idézettel.

„… a hálózatok által átszőtt globális világ sosem volt olyan sebezhető, mint manapság. Ez a sebezhetőség a nyitottságból, a bonyolult technikai rendszerekből, az infokommunikációs rendszerektől való növekvő függésből, illetve az összefonódó és egymással összekapcsolt létfontosságú infrastruktúrákból eredeztethető. Egy olyan bonyolult, infokommunikációs rendszerekkel behálózott társadalomban és gazdaságban, ahol közel minden ügyünket a hálózaton keresztül intézzük, saját fejlettségünk csapdájába eshetünk."

Forrás: [9] 95.o.

A hálózatok bonyolultsága és összetettsége megköveteli, hogy a kritikus infrastruktúra üzemeltetés kapcsán mélyebben elemezzük azt. Ennek érdekében a kritikus informatikai üzemeltetést ebből az aspektusból kívántam megközelíteni és bár az idézettek a technikai értelemben vett hálózatokat említik, a hálózatok összefüggését nem csak az informatikai, telekommunikációs hálózatok szemszögéből vizsgáltam.

Fontos még a komplex hálózatok definiálása:

„A komplex hálózatok egy meghatározás szerint nem triviális topológiai jellemzőkkel rendelkező – vagyis nem egyszerű, szabályos (pld. rács-) és nem is véletlenül kialakult – hálózatok. Más megfogalmazások szerint a komplex hálózatok olyan hálózatok, amelyek struktúrája nem szabályos, összetett és időben dinamikusan változó, a hálózattudomány célja pedig a kis hálózatok elemzése helyett a több ezer, vagy millió, köztük dinamikusan működő csomópontokból felépülő rendszerek vizsgálata."

Forrás: [8] 183. o.

Még egy nagyon fontos megállapítást tett Munk Sándor, hivatkozva egy korábban megjelent publikációra:

„Olyan fontos hálózatok, mint az Internet és a villamos-energia hálózatok egyre nagyobbak lesznek, több százmillió, vagy akár milliárdnyi csomópontot foglalnak magukban. Csomópontjaik között összetett és gyakran dinamikus kapcsolati mintázatok találhatóak. Az egyes hálózatok egymással – sokszor rekurzív módon – is kapcsolatban állnak. Társadalmi hálózatok építenek információs hálózatokra, amelyek kommunikációs hálózatokra, azok pedig fizikai hálózatokra épülnek."

Forrás: [8] 177. o.

A továbbiakban az alábbi definíciót értem hálózat alatt:

A hálózat az egymással összekapcsolt csomópontok halmaza, amelyek rendszert alkotnak. A hálózatok kapcsolatban vannak, hatnak egymásra. Ezek alapján az informatikai üzemeltetésben fontos a különböző hálózatok egymással való kapcsolódásának elemzése. Minden hálózatra jellemző a bővüléssel együttjáró tulajdonság.

1.2. RENDSZER

Az általam megfogalmazott hálózat definíciójában szerepelt a rendszer szó. Hasonlóan a hálózat meghatározásához, itt is sok mindent érthetünk alatta a különböző területek értelmezése szerint. Fontos a rendszer fogalmának meghatározása is a kritikus infrastruktúra megértéséhez.

Az internetes keresés közben találtam rá Husi Géza által összegyűjtött rendszerrel kapcsolatos meghatározás gyűjteményre. Husi Géza több definíciót is talált a rendszer általános értelmezésére és azok csoportosítását és célját határozta meg.

Így Ludvig von Bertalanffy[11] megfogalmazása szerint:

„… a rendszer kölcsönhatásban lévő elemek együtteseként értelmezhető, ahol az elemeket fizikai vagy fogalmi entitásnak (valamely dolog tulajdonságának az összessége) értelmezzük.”

Forrás: [10] 1. o.

C. West Churchman[12] szerint pedig:

„…a rendszerek olyan alkotóelemek halmazából épülnek fel, amelyek a rendszeren belül a fő célért működnek együtt. A rendszerszemléletű gondolkodás nem más, mint csupán ezekről a teljes rendszerekről és alkotóelemeikről való gondolkodási módszer.”

Forrás: [10] 3. o.

Pokorádi László a technikai rendszereket pedig a következők szerint határozta meg:

„Technikai rendszer az anyagi világ vizsgálatunk tárgyát képező része, mely egymással valamilyen kölcsönhatásban lévő elemek (berendezések és személyek) összessége. A rendszer állapota, illetve a benne lejátszódó folyamat a be- és a kimenő,

[11] Karl Ludwig von Bertalanffy (1901-1972) magyar származású osztrák biológus.
[12] Charles West Churchman (1913-2004) amerikai filozófus és rendszerkutató.

valamint a belső jellemzőkkel írható le. A környezet kölcsönhatásban lehet a rendszerrel és meghatározza a rendszer működésének peremfeltételeit."

Forrás: [11] 5. o.

A rendszerszemléletű gondolkodásom kialakulásánál ebben a definícióban megfogalmazottak voltak az irányadóak.

Nagy kérdés az is, hogy mi számít rendszerelemnek? Az önálló entitással bíró elem (pl. router) már rendszerelemnek számít, de egyben az is egy rendszer, amely tovább bontható még több részelemre (memória, tápellátás, NIC[13] stb.).

A rendszer egy szűkebb meghatározása az informatikai rendszer, amely a Magyar Honvédség Informatikai Szabályzatának kiadásáról szóló 39/2014. HM utasításának 1. számú melléklete (a továbbiakban: MH Informatikai Szabályzat) szerint:

„Informatikai rendszer – information system: eszközök, módszerek, eljárások és üzemeltető személyzet egységes irányítás alá tartozó rendszere, amelynek rendeltetése információfeldolgozási, tárolási, megjelenítési funkciók elektronikus technikai eszközökkel történő megvalósítása."

Forrás: [12] 1. melléklet 1.1.2.3. pontja

A rendszer működésére hat az őt körülvevő környezet. Nagyon fontos a környezet mint fogalom bevezetése a rendszer vizsgálatánál. Az informatikai rendszer üzemeltetését befolyásoló külső környezetre legtöbbször nincs közvetlen ráhatása az üzemeltetőknek, vagy csak minimális mértékben. Ilyenek lehetnek a jogszabályi korlátozások, természeti adottságok, nemzeti, vállalati kultúrák, elvárások stb.

Mindezeket figyelembe véve saját definícióm szerint:

A rendszer az egymással összefüggésben, kölcsönhatásban levő elemek hálózata, amelyek egy egészet alkotnak valamilyen cél érdekében. Egy elem tulajdonságának a megváltoztatása hatással lehet más elemekre és befolyásolja az egész rendszer tulajdonságát. A rendszerelemeket tartalmazó halmazon kívül eső részt környezetnek nevezzük. A rendszert és a környezetet egymástól elválasztó rész a rendszerhatár. A rendszeren belül megfigyelhetően alrendszerek, amelyek kapcsolatban állnak, hatnak egymásra. [13]

[13] NIC (Network Interface Card) hálózati kártya

1.3. INFORMATIKA – BIZTONSÁG

Az informatikai rendszerek üzemeltetése során az egyik legfontosabb szempont a biztonság. Ezért is tartom fontosnak tisztázni a biztonság, információbiztonság, üzemeltetés biztonság és az informatikai biztonság fogalmát.

Először tehát a **biztonság** fogalma általánosságban:

„A biztonság a társadalom belső viszonyaiban kifejezi azt az állapotot, amikor az egyes társadalmi alrendszerek funkciók szerint, szabályozottan működnek és működésüket semmilyen immanens veszély nem zavarja.

A biztonság a társadalom külső oldalán jelenti azt az állapotot, amikor az adott társadalom működésére más állam, szervezet, illetőleg csoportosulás veszélyt nem jelent.

A biztonság szervezeti értelmezésben jelenti azt az állapotot, amikor a szervezet egyes elemei, azok kapcsolódása, illetőleg a struktúra egésze normalizált körülmények közt funkcionál."

Forrás: [14] 148. o.

Amennyiben az informatikai rendszerek relációjában szeretném megnézni mit jelent a biztonság mint fogalom, akkor talán a következő megfogalmazás lesz használható:

„Az információ és informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik."

Forrás: [15] 190. o.

Információbiztonságnak nevezzük:

„(information security) az információk védelme a véletlen, vagy szándékos jogosulatlan megismerés, továbbítás, módosítás vagy megsemmisítés ellen. Megj.: Az információ létezhet az emberi agyban, dokumentum formában és elektronikus formában…"

Forrás: [16]

Az elektronikus információvédelem több szakterületből áll, amelyek informatikai és hálózati biztonság, átviteli biztonság, rejtjelzés és TEMPEST[14].

[14] TEMPEST eredetileg kódszó, az elektronikai eszközök kisugárzásának elemzésére, napjainkban a kompromittáló kisugárzás elleni védelmet jelenti.

Az **informatikai biztonság** pedig:

„Az informatikai biztonság a védelmi rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.”

Forrás: [17] 2. rész 4. fejezet 40. o.

Értelmezésem szerint egy informatikai rendszer biztonságos üzemeltetése esetében éppen olyan fontos a rendszerüzemeltetés biztonsága, mint egyéb más összetevők, amelyek az információbiztonságból adódnak. A fenti definíció szerint fontos a rendszer működőképességét, az információk elérhetőségét, sértetlenségét és megbízhatóságát biztosítani, melyhez elengedhetetlen a megfelelő és biztonságos üzemeltetési feltételek biztosítása.

Üzemeltetés biztonság az informatikai rendszerek zavartalan működőképessége és rendelkezésre állása érdekében betartott előírások, rendelkezések és szabályok összességét jelenti. A fő cél a folyamatos működés fenntartása, amely egyes esetekben az informatikai biztonsággal ütközhet, összességében azonban annak a szerves része.

Az értekezésemben az üzemeltetés biztonságot a fenti megfogalmazás szerint használom.

Gyakran találkozhatunk az angol „CIA” rövidítéssel, amely az elektronikus információbiztonság alapjául szolgál. Ahol a „C” a Bizalmasságot (Confidentiality), a „I” a Sértetlenséget (Integrity), az „A” pedig a Rendelkezésre állást (Availability) jelenti. Ezen három alapfogalom szervesen kapcsolódik egymáshoz és csak együttesen biztosítják a komplex IT biztonságot. [18] [19]

Bizalmasság (C)

A rendszerben tárolt és hozzá kapcsolódó adatokhoz és szolgáltatásokhoz kizárólag az arra jogosultak férhetnek hozzá. A hozzáférés módja szintén szabályozott körülmények között történik. [18] [19]

Sértetlenség, integritás (I)

A sértetlenség alatt azt értjük, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, továbbá az elvárt forrásból származnak (hitelesség) Abban is biztosak lehetünk, hogy az adat valóban létezik (letagadhatatlanságát), azt egy adott valaki, valami írta, módosította vagy megismerés történt (elszámoltathatóság). [18] [19]

Rendelkezésre állás (A)

A jogosult számára az elektronikus információs rendszer elérhető és az elvárt módon használható. A rendelkezésre állás megmondja, hogy milyen követelmény támasztható a rendszerrel szemben, figyelembe véve az informatikai infrastruktúra képességeit. A felhasználóknak tisztában kell lenni, hogy a rendszer esetleg nem lesz mindig elérhető, ugyanakkor biztosítva van a maximális leállási idő is, amely után a szolgáltatásoknak újra elérhetőnek kell lenniük. Megfelelő szintű kockázatkezeléssel megnövelhető a rendelkezésre állás. Eljárásokkal és komoly anyagi ráfordításokkal a rendelkezésre állást közelíteni lehet a 100%-hoz. [18] [19] [20]

Ugyanakkor a rendelkezésre állás szempontjából nem mindegy az sem, hogy a leállások milyen gyakran következnek be. Lehet, hogy többször rövid ideig tart, vagy ritkábban következik be, de akkor hosszabb ideig elhúzódik. Amennyiben ezek tervezett leállások (pl. karbantartás miatt) nem feltétlenül jobb vagy rosszabb az egyik a másiknál, attól függ, hogy ez milyen üzemeltetési környezetben következik be. Egyszer az a követelmény, hogy nagyobb leállásokkal történjen a karbantartás, máskor a többszöri rövidebb idő az előnyösebb.

Az üzemeltetés szempontjából az informatikai biztonsági előírások külső befolyásoló tényezőként is értelmezhetők, mert eszerint is kell elvégezni a feladatokat, illeszkedni kell az üzemeltetési szabályzatnak a biztonsági dokumentumokhoz.

1.4. A KRITIKUS INFRASTRUKTÚRA

Miután tisztáztam a hálózat, a rendszer fogalmát meg kell határoznom a kritikus infrastruktúra fogalmát is, amiért létrehozzák a kritikus informatikai rendszert.

„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."

Forrás: [21] 3.2. pont

A fenti kormányhatározat a kritikus infrastruktúra fogalmat használja, ami nemzetközi „Critical Infrastructure" kifejezésből ered. A magyar jogszabályalkotás a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény már létfontosságú rendszernek nevezi a kritikus infrastruktúrát, amely alapján:

„meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna, …"

Forrás: [22] 1. § f) bekezdés

Magyarországon az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényben az alábbi ágazatok kerültek besorolásra: Energia, Közlekedés, Agrárgazdaság, Egészségügy, Pénzügy, Infokommunikációs technológiák, Víz, Jogrend – Kormányzat, Közbiztonság – Védelem, Honvédelem.

1.5. KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA

2007-ben Muha Lajos doktori értekezésében elemezte a hazai és a nemzetközi szervezetekben és országokban meglévő kritikus információs infrastruktúra fogalmakat, majd saját definíciót fogalmazott meg:

„Azon az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek

működésképtelenné válása vagy megsemmisülése a kritikus infrastruktúrák működésképességét jelentősen csökkentené."

Forrás: [23] 40. o.

Létfontosságú információs rendszert és létesítményt (Kritikus Információs Infrastruktúra) 2013-ban a magyar jogalkotók a következők szerint fogalmazták meg:

„a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek."

Forrás: [24] 1. § f) bekezdés

A jogszabályi meghatározásból talán a környezettel való kapcsolódása hiányzik, amely az általam meghatározott rendszer definíciójában megtalálható. Tisztán látszik azonban a hálózat és a rendszer vizsgálatának a fontossága. A fenti definícióból is kitűnik, hogy egyes kritikus infrastruktúra elemek mennyire fontosak az adott ország működése szempontjából. [25]

1.6. KRITIKUS INFORMATIKAI RENDSZER

Az előző fogalmakat is figyelembe véve a kritikus informatikai rendszer alatt az értekezésben a következő definíció szerint használom:

Kritikus informatikai rendszer az egymással összefüggésben, kölcsönhatásban levő informatikai rendszerelemek hálózata, amelyek egy egészet alkotnak és az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek. Egy elem tulajdonságának a megváltoztatása hatással lehet más elemekre és befolyásolja az egész informatikai rendszer tulajdonságát. A rendszerelemeket tartalmazó halmazon kívül eső részt környezetnek nevezzük, amellyel kölcsönhatásban van az informatikai rendszer.

Az értekezésemben kritikus informatikai rendszert az üzemeltetés biztonsági oldaláról és üzemeltetési szemszögből vizsgálom. Részletesebben az adatközpontokat elemzem.

1.7. ADATKÖZPONT

Az egységes értelmezés érdekében még fontosnak tartom leírni az adatközpont definícióját. Az IVSZ Adatközpont és Felhő Munkacsoport az alábbi megfogalmazást használja:

„*Informatikai és távközlési infrastruktúra biztonságos és hatékony elhelyezését, működtetését szolgáló technológiai rendszereket magában foglaló cél-létesítmény.*”

Forrás: [26] 4. o.

A fenti definíció megfelel az értekezésemben használt értelmezéssel.

1.8. ÖSSZEGZÉS

A fejezetben tisztáztam az értekezésem szempontjából meghatározó definíciókat, amely szükséges volt a kutatásom elvégzéséhez. Ezen kívül új definíciókat alkottam, a meglévőket pontosítottam a hálózat, üzemeltetés biztonság és a rendszer tekintetében. A definíciók alkotása, illetve pontosítása, annak érdekében történt, hogy az értekezésemben a leírtakat egységesen lehessen értelmezni. A hálózat és a rendszer fogalmának tisztázására azért is volt szükség, mert aszerint, hogy milyen környezetben van használva más és más definíciót használnak rá.

Az értekezésemben a rendszer az egymással összefüggésben, kölcsönhatásban levő elemek hálózata, amelyek egy egészet alkotnak valamilyen cél érdekében. Egy elem tulajdonságának a megváltoztatása hatással lehet más elemekre és befolyásolja az egész rendszer tulajdonságát. A rendszerelemeket tartalmazó halmazon kívül eső részt környezetnek nevezzük. A rendszert és a környezetet egymástól elválasztó rész a rendszerhatár. A rendszerszemléletű gondolkodásom kialakulásánál ebben a definícióban megfogalmazottak voltak az irányadóak.

Üzemeltetésbiztonság alatt az informatikai rendszerek zavartalan működőképessége és rendelkezésre állása érdekében betartott előírások, rendelkezések és szabályok összességét értem. A fő cél a folyamatos működés fenntartása, amely egyes esetekben az informatikai biztonsággal ütközhet, összességében azonban annak a szerves része.

Értelmezésem szerint a kritikus informatikai rendszer az egymással összefüggésben, kölcsönhatásban levő informatikai rendszerelemek hálózata, amelyek egy egészet alkotnak és az információ folyamatos biztosítása és az informatikai

feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek. Egy elem tulajdonságának a megváltoztatása hatással lehet más elemekre és befolyásolja az egész informatikai rendszer tulajdonságát. A rendszerelemeket tartalmazó halmazon kívül eső részt környezetnek nevezzük, amellyel kölcsönhatásban van az informatikai rendszer.

A definíciók értelmezése, mélyebb megismerése megerősítette bennem azt a gondolatot, hogy a biztonságos üzemeltetésnek egyik alappillére az üzemeltetés biztonság magas színvonala. Ez egy másfajta megközelítése a témának. Belülről kifelé elemzem az eseményeket, míg, ha valaki az információbiztonság oldaláról közelíti meg a területet, akkor ő kívülről befelé teszi ugyanazt. A siker véleményem szerint a két vizsgálati módszer együttes alkalmazásával érhető el.

A kritikus infrastruktúrát egy kormányhatározat definiálta 2012-ig, amely évben megjelent törvény már mint létfontosságú rendszert említi.

A kritikus információs infrastruktúra a létfontosságú rendszerek kiszolgálására szolgáló eszközök és módszerek összessége. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. Korm. rendeletben megfogalmazott definíciót kiegészítettem. Erre azért volt szükség, mert a rendelet nem tartalmazza a környezeti hatásokat. Az általam használatos rendszer meghatározásában azonban szerepel és véleményem szerint egy nagyon fontos eleme annak.

2. HÁLÓZATELMÉLETI ALAPOK

A kutatásom megkezdésekor fontosnak tartottam megismerni a hálózatelmélet alapjait, hogy jobban átlássam az összefüggéseket, megértsem a rendszerelemek hogyan kapcsolódhatnak egymáshoz és milyen törvényszerűségek figyelhetők meg egy hálózat életében. A deduktív kutatási módszer alkalmazásával az általános hálózatelméleti megállapításokat már összehasonlíthattam az informatikai rendszert alkotó hálózatokkal. Fontosnak tartottam a gráfok, mátrixok, egyéb matematikai alapok megértését annak érdekében, hogy a kutatásom során feltárhassak olyan hálózatelméleti törvényszerűségeket, amelyeket enélkül nem tehettem volna meg. A hipotézisem szerint ezek az elméleti alapok fogják később megalapozni egy döntéstámogató rendszer[15] algoritmusait. Annak érdekében pedig, hogy a számítógéppel feldolgozhatók legyenek a folyamatok és az eszközök paraméterei, a valóságot a modellezés segítségével kell adatokká alakítani. A modellalkotási folyamatok elméleti alapjai így szintén elengedhetetlenek, amennyiben egy szoftver létrehozatalához szeretnék kritériumokat meghatározni.

A világban egymástól függetlenül, vagy éppen összekapcsolva több ezer hálózattal találkozhatunk. A bonyolult felépítés feltérképezésére már ma is léteznek szoftverek, amelyek adatbázisok, adattárházak, dokumentumok, képek alapján képesek grafikus megjelenítést végezni, amely átláthatóbbá teszi a sokszor rendkívül szövevényes kapcsolatrendszereket. Ennek segítségével ki lehet szűrni a dezinformációkat, összefüggéseket lehet feltárni, előrejelzéseket, algoritmusokat lehet készíteni. A különböző nézetek (időrend, sok kapcsolattal rendelkezők, vagy éppen a kevés, de fontos kapcsolatokkal rendelkezők kiemelése) segítenek rávilágítani elrejtett fontos tényezőkre. [27]

Ebben a fejezetben a hálózatelméleti alapokat és a mátrix alaptételeit mutatom be – a részletesség mellőzésével –, hogy könnyebben belátható legyen, milyen nagy lehet a haszna a hálózatkutatásnak mint tudománynak a kritikus információs infrastruktúra üzemeltetésének támogatásában.

A megismerésnek az egyik legfontosabb része az adatok begyűjtése, a valós kép modellezése.

---

[15] Az értekezésemben a „döntéstámogató rendszer” fogalmat és a „felügyeleti és beavatkozó rendszer” fogalmat felváltva használom, de ugyanazt értem a kettő alatt.

2.1. MODELLEZÉS

Az olyan rendszer vizsgálatához, ahol a rendszerelemek bonyolult hálózatba vannak kapcsolva a hálózatelméletet kell segítségül hívni. A kapcsolatok által a kölcsönhatásokat, a mozgásokat, a viselkedést tudjuk leírni egy matematikai szempontból feldolgozható formában. A különböző rendszerekről felírt „modellek" hasonlóságot mutathatnak, amelyekből szabályszerűségekre következtethetünk.

„A modell egy valóságos rendszer egyszerűsített, a vizsgálat szempontjából lényegi tulajdonságait kiemelő mása. A modell mindazon másodlagos jellemzőket elhanyagolja, amelyeket a kitűzött vizsgálat szempontjából nem tekintünk meghatározónak. Ezért elég, ha a modell a valódi rendszert csak a meghatározott szempontból vagy szempontokból helyettesíti. Sőt, a vizsgálat szempontjából lényegtelen szempontok figyelembevételé kifejezetten káros. Bonyolítja magát a modellt és igy a vizsgálatot, de lényegi információhoz nem jutunk vele."

Forrás: [11] 26. o.

A modellezéssel a valóságot képezzük le, de soha nem a teljes részletességében mutatjuk be, főleg nem egy életciklusát az adott dolognak. Az egyik legnehezebb feladat, hogy mit hagyhatok ki a modellalkotásból és mi az, amit mindenképpen szerepeltetnem kell. [13] [28]

A számítógépes feldolgozáshoz le kell fordítani a valóságot a matematikai, majd a számítógép számára is érthető, feldolgozható információkká. Az előzőekben bemutatottak alapján, gráfokkal írjuk le a rendszert. A csomópontok lehetnek az elemek, amelyek önálló entitással rendelkeznek, kellően egyszerűek a vizsgálat szempontjából. Ezeket összekötő kapcsolatot, állapotváltozást pedig a gráf élei írják le.

A másik terület a fordított eset, amikor a modellekből alkotjuk meg a valóságos rendszert. Ezt is kell alkalmazni az üzemeltetés során, így nem a kiépítés után tapasztalunk rendellenességeket, hanem a modelleken játszunk le különböző elképzelt szituációkat. Ez a módszer több területen is megfigyelhető például a következő idézet is ezt mutatja be:

„Tehát a biológiai elvek (felépítési és működési elképzelések) alapján megalkottak bizonyos matematikai jellegű modelleket. Ezeket elméleti matematikai módszerekkel pontosították, alkalmazott matematikai (numerikus, operációkutatási, statisztikai) módszerekkel számításokra alkalmassá tették, majd számítógépen realizálták.

Azonban a matematikai módszerek mellett sokszor heurisztikus meggondolásokra és számítógépes kísérletezésre is szükség van.”

Forrás: [29] 1. o.

A rendszer és környezete szempontjából fontos a komplex rendszer vizsgálata. Mint az Arisztotelészi idézet szerint is, az egész több mint a részek összege, így a különböző rendszerelemek mutathatnak teljesen eltérő viselkedést, mint a többi vagy éppen a rendszer egésze, de fontos, hogy minden egyes rendszerelem hozzájárul a rendszer viselkedéséhez.

A számunkra rendezett rendszerek hierarchikusan épülnek fel. Azonban a valóságban az elemek bonyolult hálózatot alkotnak, amelyek kölcsönhatásba lépnek egymással. A kialakult komplex rendszerek egyes alrendszereinek működése a teljes rendszerre úgy hat, hogy az megváltoztatja a rendszer alapvető működését. Ilyenek pl. a turbulens áramlások, amelyeket különböző irányú és sebességű örvények alkotják, amiből kialakul.

A komplex rendszerekre jellemző tulajdonság a spontán szerveződés, amely külső beavatkozások nélkül jön létre. Kialakul egy új, a rendszerre jellemző, annak tulajdonságát meghatározó felépítés. A természetben a hókristályok kialakulására jellemző folyamat, hogy a folyadékból a kristályszerkezet kialakulása között megfigyelhető az pont, mikor a rendezetlen állapotából a rendszer a rendezett állapotot veszi fel. Általában ez a fázisátalakulási pont jellemző a komplex rendszerekre, ahogyan a „káosz” határán mozognak. [30]

A káosz természetéről írt egy cikkében Tél Tamás és Gruiz Márton. Ebben azt mondják, hogy a kaotikus rendszerekben az előrejelezhetetlenség korlátozott, csakis a kaotikus attraktoron áll fenn. Ezek szerint a pillangó[16] szárnymozgásából kialakuló tornádó nem minden esetben, csak akkor történhet meg, ha a szárnycsapás keltette mozgáspálya rajta van az attraktoron. [31]

Egyrészt ez számomra azt is jelenti, hogy márpedig meg is történhet ez a jelenség, másrészt jelen esetben nekem csakis a szemléltetés érdekes. Tehát a rendszerünkben bármilyen kis esemény kiválthat komoly problémákat. Amennyiben hozzávesszük a kritikus infrastruktúráknál számbavehető dominó effektust, ez igenis komoly gondokat okozhat. A későbbiekben éppen ezért is tartom fontosnak leírni, hogy

[16] A pillangóhatás a nevét a pillangó szárnyának csapásáról kapta, amely kelthet olyan szelet, ami akár tornádóhoz vezethet.

a lehető legtöbb információt rögzítenünk kell a rendszerünkről, amelynél nem csak statikus, de dinamikus viselkedés is érdekes lehet. Nehéz meghatározni azt a mennyiségű betáplált adatot, amellyel elég pontosan lehet modellezni a rendszert, de nem olyan sok, hogy a feldolgozásra fordított idő beláthatatlan ideig tartson.

Erre a legszemléletesebb példa az időjárás előrejelzés. Az időjárás változását nehéz rövid idő alatt megjósolni, mert több egymástól látszólag független dolog hat egymásra, melynek hatásai vagy összeadódnak, vagy kioltják egymást. A rendszer elemek modellezésére nagy számításkapacitással bíró szervereket használnak, azonban ezek is sokszor lassabban számolják ki a lehetséges időjárást, mint az bekövetkezik. Amennyiben a számítógépek olyan sok ideig dolgozzák fel a betáplált adatokat, hogy már a kinyert információval nem tudunk semmit kezdeni, mert az előre jelzett idő eltelik. Egyrészről törekedni kell a minél több információ összegyűjtésére, amellyel minél aprólékosabb és több számítást tudunk elvégezni, így pontosabb eredményeket kaphatunk. Ugyanakkor a rendelkezésre álló sok adatnak hátránya is van, mert nagyon lassú és ebből adódóan tovább tart az előrejelzés, valamint kellően bonyolult rendszer esetén rohamosan nő a hibalehetőség. Ezeket figyelembe véve azonban, rengeteg szenzort kell alkalmazni és még ennél is több számítást kell elvégezni. A negyedik fejezetben tárgyalt döntéstámogató rendszernél is kihívást jelent hol húzzuk meg a határt. Rögzíteni kell a sérülékenységet, a fenyegetettségeket, a vagyonelemek jellemzőit és az alapadatokat. Ezeket tapasztalati úton, gyártóktól, szenzorokból és egyéb helyekről is összegyűjthetjük. Ez nagyon nagy munka és a ráfordított energia nem biztos, hogy megéri, de a következő gondolat kritikus információs infrastruktúrára átültetve talán rávilágít arra miért is szükséges megtennünk. [13]

„Az éghajlat modellezése nehéz, és bizonytalanságok kísérik. Ám az, hogy bizonytalanok vagyunk abban, hogy miként reagál az éghajlat a többlet üvegházgázokra, nem igazolhatja a tétlenkedést. Ha egy gyors motorkerékpárral, sűrű ködben egy sziklaszirt pereme közelében hajtunk, de nem áll rendelkezésünkre a sziklaszirt pontos térképe, akkor a térkép hiánya felment-e az ésszerűen elvárható lassítási kötelezettség alól?”

Forrás: [32]

A csomópontok leírása szempontjából beszélhetünk diszkrét és folytonos értékekről. A folyamatos jelnél az idő minden értékére értelmezhető (pl. analóg jel), a diszkrétnél csak egyes időpillanatokban vett jeleket értelmezzük, ilyenek az analóg jelek

a digitalizálást követően. Beszélhetünk még intenzív és extenzív értékekről. Az intenzív értékek nem összegezhetőek, az extenzívek pedig összegként jeleníthetőek meg. Fontos fogalom még a sztochasztikus és a determinisztikus jel. Determinisztikus jelfolyamról beszélünk, ha minden időpillanatban egyértelműen meghatározható a jel értéke, sztochasztikus, ha nincs ismeretünk minden időben a jelről. Ekkor a modell nem pontos. Ahhoz, hogy a valósághoz közelítsen a modellünk valószínűségszámítást és statisztikai módszereket kell alkalmazni. A két típusú jelsorozat a gyakorlatban egyszerre jelenik meg a rendszerek vizsgálata során, gondoljunk a hasznos jel és a zaj együttes jelenlétére. A tökéletes az lenne, ha analóg jelet tudnánk feldolgozni, mert vagy túl sűrűn veszem a jelet és akkor közelítek a valósághoz, de ekkor túl sok adatot kell feldolgozni, vagy kevés a minta, de akkor pontatlan lesz a modell. [11] [13]

A nagy rendszerek modellezésére, ahol sok bizonytalansági tényezővel találkozunk kiválóan alkalmazható a Fuzzy modellezés. A kockázatkezelési eljárásoknál ez a fajta modellalkotás gyors számítógépekkel feldolgozható kockázatbecslési számításokkal segíti a döntéshozatali folyamatokat. Az alkalmazása során valamilyen kvalitatív eljárást alkalmaznak. Az ISO/IEC [17] 27005 szabványban [18] jól ismert Kockázatbecslési Mátrixot felhasználjuk, amely a kockázat súlyosság és valószínűségét írja le. Ebből megalkotjuk a kockázati kategóriák tagsági függvényeit. Majd ezt követően a rendszer a bemenő jellemzőinek pillanatnyi értékeihez egy-egy fuzzy tagsági értéket rendelünk. A fuzzyfikációval kapott eredmények alapján megállapítható a veszély súlyossága, az esemény bekövetkezésének valószínűsége. Ez után már logikai kapcsolatokkal feldolgozható a rendszerben bekövetkező változás. A rendszer automatikus riasztásokat adhat, illetve be is avatkozhat. [11]

A kaotikus rendszerekben az előrejelezhetetlenség korlátozott, ezért törekedni kell ezt az állapotot elkerülni. Egyrészt minden információt össze kell gyűjteni, másrészt kerülni kell a spontán dolgokat. Nagyon fontosnak tartom a szigorú szabályozást, a szabályozott strukturális felépítést.

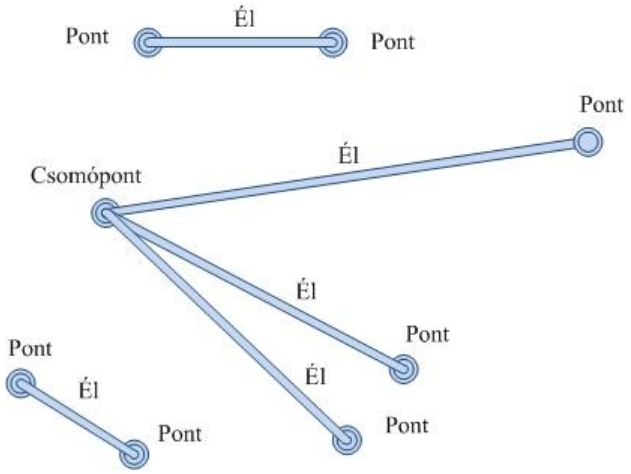
[17] ISO (International Organization for Standardization) Nemzetközi Szabványügyi Szervezet; IEC (International Electrotechnical Commission) Nemzetközi Elektrotechnikai Bizottság
[18] ISO/IEC 27005 Információbiztonsági kockázatmenedzsment.

2.2. GRÁFOK

A gráfokkal kapcsolatban a mélyebb matematikai ismereteket mellőzve tisztáznom kell néhány alapfogalmat ahhoz, hogy a hálózatok működésébe beláthassunk. A hálózat szerkezetét, tulajdonságát és viselkedését matematikailag gráfokkal tudjuk leírni, ezáltal vizsgálni is. Mint hogy egy új területről van szó folyamatosan változtak a vizsgálati módszerek. Kőnig Dénes[19] 1936-ban írta meg a gráfelméleti tankönyvét, amely a magyar hálózatkutatás korai szakaszában rendszerezte a témával kapcsolatos ismereteket.

„A hálózat fogalma a hálózattudományban matematikai, ezen belül gráfelméleti alapokra épül. Ennek megfelelően a hálózat csúcsok/csúcspontok (csomópontok) és az ezeket páronként összekapcsoló élek (kapcsolatok) összessége. Az ezzel lényegében megegyező tartalmú gráf fogalom azonban csak a hálózatok legegyszerűbb változatainak leírására alkalmas.”

Forrás: [8] 182. o.



1. ábra Hálózat – gráf
(saját szerkesztés)

A **gráf jelölése**:

G= (V, E, Ģ), ahol a:

V[20] a pontokat (más néven csomópontok, amikor több él találkozik),

E[21] az éleket, Ģ a leképezést jelöli.

(1) Forrás: [33] 1151. o.

[19] Kőnig Dénes (1884-1944) magyar matematikus
[20] Angol vertex= csúcs szóból (A magyar jelölésnél a V helyett sokszor a P jelölést használják)
[21] Az angol edge = él szóból

Irányítatlan gráfnak is nevezik, mert nem vizsgálják, hogy a két pontot összekötő él milyen irányba mutat.

Csomópontok számának jelölése: $n = |V|$

Élek számának jelölése: $e = |E|$

Abban az esetben, ha fontos az élek iránya, akkor **irányított gráf**okat használunk.

A jelölése:

$$\vec{G} = (V, \vec{E})$$

(2) Forrás: saját

Ilyenkor az **élek jelölése**: e= (u, v), ami azt jelenti, hogy u-ból kiindulva v-be jutunk az adott élen keresztül.

Ha egy egyszerű gráf bármely két pontja össze van kötve éllel, akkor **teljes gráfnak** nevezzük.

Egy csomóponthoz csatlakozó élek számát **fokszám**nak nevezzük. Ez egy nem negatív egész szám. Lehet nulla is, ami akkor fordul elő, amikor a pont nem kapcsolódik éllel egy másik ponthoz. A v ∈ V csúcs fokszámát d(v)-vel jelöljük.

Azt, hogy egy gráfban amilyen gyakorisággal fordulnak elő a különböző fokszámú csúcspontok **fokszámeloszlásnak** nevezzünk.

A gráf megrajzolásakor a csomópontok térbeli elhelyezkedése közömbös, így a pontok áthelyezésével egy számunkra áttekinthetőbb rajzot is kaphatunk. **Izomorfnak** nevezünk két gráfot, ha az egyik csúcsai leképezhető a másikban és azokat pontosan akkor köt össze él, ha a másikban is összekötötte. Minimális feltétele a fokszám azonosság. [6] [33] [34] [35]

A következő lépésben már nem csak a két csomópont közötti kapcsolatot vizsgáljuk, hanem több csomópont kapcsolatát is egymással. Akkor **összefüggő** egy **gráf**, ha bármelyik két pont között létezik folyamatos séta. A gráfelméletben a **séta** azt jelenti, hogy az összekapcsolt pontok és a csomópontok váltják egymást. Erősen összefüggő, ha irányított gráfok esetében is igaz, hogy bármelyik két pont esetén eljuthatunk egyikből a másikba. A **hálózat sűrűsége** megmutatja a létező és a lehetséges összes él arányát. **Útnak** nevezzük azt a sétát, amikor egyetlen ponton és élen sem haladunk át egynél többször. **Vonal**ról akkor beszélünk a gráfelméletben, amikor egy séta során az éleket csak egyszer érintjük, de a pontokon többször is

áthaladhatunk. Az összefüggő részgráfokat **komponenseknek** hívjuk. Az összefüggő gráfnak azt az élét, amelynek törlésével több komponensre hullik **hídgráfnak** nevezzük. Amennyiben az embereknek a kapcsolati hálóját vizsgálom, akkor nyilván a közöttük lévő kapcsolatot jelölik az élek. Amikor az alkalmazások közötti kommunikációt elemzem, akkor az élek ezeket a kapcsolatokat jelölik. Ez két külön hálózat, de a két hálózat összeköthető híd gráfokkal. Megteremthető az ember-technika-környezet kapcsolata, tehát létrehozható egy többrétegű hálózati struktúra. [33]

Töréspontnak pedig azt a csomópontot hívjuk, amelynek a törlésével szintén széthullik a gráfunk. [6] [33] [34] [35]

Fontos terület az a súlyozott gráfok gyakorlati alkalmazásánál, amikor azt keressük, hogy mi a minimális kiépítési költsége egy fizikai IT hálózatnak, csővezetéknek, villanyvezetéknek stb., ahol el kell érni minden pontot a hálózatban. Természetesen minden csomóponthoz legalább egy élnek kell kapcsolódnia. [36]

Több gráfbejáró algoritmus is létezik. Ezekkel például megtalálhatjuk egy kezdőpontból egy másik tetszőleges pontba vezető legrövidebb utat (a szociológiában ezt a számot **elérhetőségi mutatónak** hívják).

Néhány algoritmus:

- Dijkstra algoritmus[22];
- Bellman-Ford-algoritmus[23];
- Floyd algoritmus[24];
- Warshall algoritmus[25].

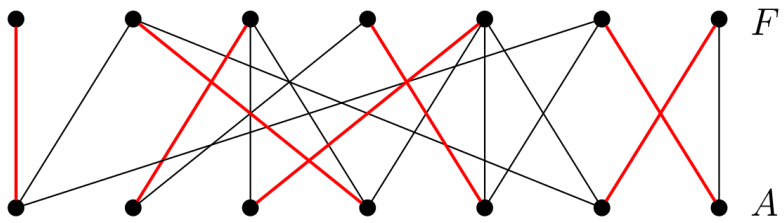
Sokszor valamilyen előnyös tulajdonságú csomópontot keressük, amelyet a „legjobbat-először” módszernek nevezünk. Ehhez a kereséshez nyújt segítséget az A* algoritmus.[26] [37]

A Gráfoknak egy számomra érdekes tulajdonsága a Matematika című könyvben található. [33]

[22] Edsger Wybe Dijkstra (1930–2002), holland matematikus és informatikus.
[23] Lester Randolph Ford (1886-1967) amerikai matematikus, Richard Ernest Bellman (1920-1984) amerikai alkalmazott matematikus.
[24] Robert W. Floyd (1936–2001) amerikai informatikus.
[25] Stephen Warshall (1935-2006) amerikai informatikus.
[26] Amerikai IT tudósok által létrehozott: Bertram Raphael (1936-), Nils Nilsson (1933-) és Peter Hart (1940-).

„Egy gráfot párosnak mondunk, ha csúcsainak halmazát két diszjunkt részhalmazra bonthatjuk úgy, hogy élek legfeljebb két különböző részhalmazba tartozó csúcsok között futnak, míg az egy részhalmazba esők között nincsen él.”

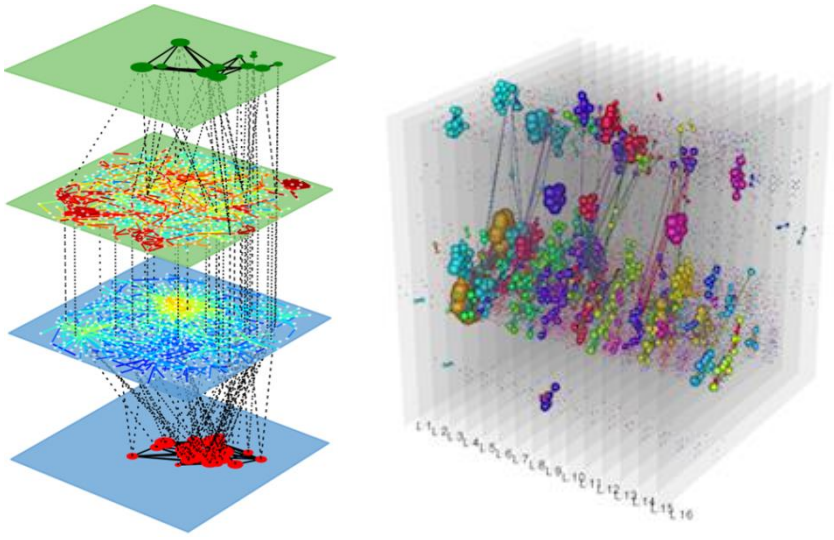
Forrás: [33] 1174. o.



2. ábra Páros gráf *[214]*

Amennyiben az „F” az informatikai rendszerünk felhasználóit és „A” az eltérő alkalmazásokat jelöli, akkor a közöttük lévő élek megmutatják, kinek milyen alkalmazáshoz lehet hozzáférése. Ez egy kapocsszerkezet lehet az emberekből álló hálózat (halmaz) és a technika, (vagy alkalmazások) alkotta hálózat között.

A 3. ábra szemlélteti, hogy a hálózat különböző rétegei hogyan kapcsolódnak egymáshoz, ezáltal olyan kapcsolódási élek jelennek meg, amelyek a többdimenziós vizsgálat nélkül nem lennének láthatóak, így ezáltal téves következtetéseket vonhatnánk le. Jelenlegi módszerekkel csak az egy szinten lévő kapcsolatokat szokták vizsgálni. Az újfajta megjelenítés segítségével a többdimenziós modellekből csökkentett, egyszerűbb modelleket hozhatunk létre, amelyek könnyebben kezelhetők.



3. ábra Többdimenziós hálózatok kapcsolata [38]

A különböző rétegek reprezentálják a hálózatukat, amelyek, mint látható nem csak a saját rétegen belüli kapcsolódásokat mutatják, hanem a többivel való összeköttetést is. Az egyik réteg lehet az IT hálózat, a másik az emberek, a harmadik a jogszabályok, a negyedik a kommunikációs hálózat stb. [39]

Vizsgálni kell, hogy számunkra különbözőnek gondolt rendszerek hogyan kacsolódnak egymáshoz a társadalmi hálózatok miként befolyásolják az elektronikai hálózatokat, és fordítva mi történik. Nem feltétlenül azt a rendszert kell vizsgálnunk, amelyiken jelenleg számíthatunk támadásra, hanem az azzal kapcsolatban lévő rendszerekben is vizsgálatokat kell folytatni. Kontroll alatt kell tartani a kapcsolódó hálózatokat is, amennyiben lehetőségünk van erre.

Jelenleg is léteznek akár ingyenes matematikai többdimenziós elemző programok. Ilyen például a MuxViz[27], ami jelenleg nincs integrálva az informatikai üzemeltetésbe bevont alkalmazásokba. **Javaslom ezen szoftverek alkalmazását, beintegrálását a kritikus információs infrastruktúrák üzemeltetése során.** Ennek segítségével megjeleníthetjük az adatbázisba rendezett és/vagy a szenzorok által rögzített adatokat, összefüggéseket. **A 4. fejezetben javaslatot teszek egy döntéstámogató rendszer kiépítésére, amelybe integrálva az említett többdimenziós hálózatokat elemző szoftvert, az elméleti kutatásokat is felhasználva lehetőség nyílik az adatok közti kapcsolódás szélesebb körű elemzésére.**

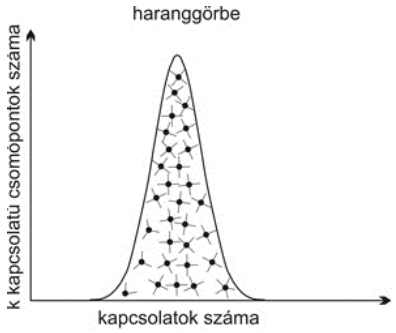
A H1 hipotézisem helyesnek bizonyul, mert a többdimenziós hálózatelméleti alapok alkalmazása egy számítógépes adatfeldolgozás során az előbb bemutatottak szerint új kapcsolatrendszereket tárhat fel, mellyel biztonságosabb és komplexebb informatikai rendszerüzemeltetést tesz lehetővé.

Az eddig leírt leképezésnél azt feltételeztük, hogy a hálózatok statikus állapotúak, vagy csak egy idő pillanatban vizsgáltuk a felépítésüket. Az életben azonban az idő változásával a legtöbb hálózat is változik. Erdős Pál[28] és Rényi Alfréd[29] a hálózatok véletlenszerű eloszlása témakörben végeztek kimagasló kutatásokat.

Barabási Albert-László[30] és kutatócsapata azt vizsgálták, hogy mi történik, ha a pontok ugyan továbbra is statikusak, de az éleket folyamatosan adjuk hozzá a pontok halmazához. Például egy általános iskolás osztály első napján a gyerekek még soha nem

[27] The Multilayer Analysis And Visualization Platform: http://muxviz.net/index.php [223]
[28] Erdős Pál (1913-1996) magyar matematikus.
[29] Rényi Alfréd (1921-1970) magyar matematikus.
[30] Barabási Albert László (1967-) fizikus, hálózatkutató.

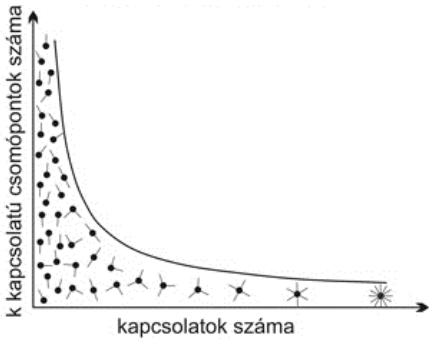
látták egymást és elkezdenek egymásnak bemutatkozni, egymást megismerni. A gyerekeket csomópontokkal jelöljük és minden egyes megismerkedést egy éllel. Ezekben a hálózatokban azt feltételezzük, hogy a pontok adottak, azok száma és tulajdonsága nem változik a vizsgálat alatt. Továbbá azt is feltételezi, hogy a statikus pontok mind ugyanolyanok, nincs közöttük kitüntetett szereppel bíró. Egy ilyen pontokból álló hálózat kialakulásának vizsgálatánál egyenrangú csomópontokat találunk. A közöttük lévő élek véletlenszerűen adódnak hozzájuk. Eszerint, ha feltételezünk egy kellően hosszú időt, akkor a pontok fokszáma azonos lesz. A fokszámeloszlást tekintve egy Poisson-eloszlást mutat. [40]



4. ábra Poisson-függvény [40] *1300. o.*

A 4. ábran az látható, hogy a csomópontok többségének közel ugyanannyi éle van. Minél több élt adunk hozzá, annál kevesebb lesz annak a valószínűsége, hogy marad olyan pont, aminek nem lesz egyetlen éle sem. Erdős és Rényi azt figyelték meg, hogy amennyiben a hálózatunkban lévő pontokra jutó élek száma meghaladja az egyet, akkor a hálózatból kimaradó pontok száma exponenciálisan csökken. Ez fordítva is igaz, amennyiben ez az érték lecsökken egy alá, a hálózatunk szétesik és sok kizárólag csak önmagukkal kommunikáló hálózatok maradnak. A valóságban például az azonos méretű városokhoz közel azonos számú út csatlakozik. [6] [40]

Azonban a valóságban nagyon kevés hálózatot írhatunk le véletlen modellekkel. Az előző példánál maradva vannak félénk gyerekek és vannak vagányabbak, akik gyorsabban teremtenek kapcsolatot. Lehet lesz olyan gyerek, aki az egész nyolc év alatt csak egy két gyerekkel barátkozik majd, de ott van az osztályfőnök, aki minden gyerekkel kialakít egy jó kapcsolatot. Legtöbb esetben az élek nem véletlenszerűen csatlakoznak a meglévő pontokhoz.



5. ábra Hatványfüggvény-eloszlás [40] *1300. o.*

Az így kialakult skálafüggetlen hálózatokban a fokeloszlás már hatványfüggvénnyel jellemezhető. Itt az figyelhető meg, hogy a pontok többségének a fokszáma kicsi és csak néhány rendelkezik több éllel. Ezek a jellemzők a gyakorlatban megfigyelhetők a repülőtér és a repülési útvonalak tekintetében. A sok éllel rendelkező csomópontokat középpontnak nevezzük. Ilyen középponttal rendelkezik a világháló is. Az internetet nézve is nagyon sok olyan router van, amelynek kevés kapcsolódási pontja van (pl. otthoni routerek), de van egy kevés (pl. az internet szolgáltatóké), amelynek nagyon sok kapcsolódási pontja van. [40]

A skálafüggetlen természetes hálózat például az ember esetében az idegrendszer, az érhálózat, a társadalmi felépítettség, de ezzel a modellel vizsgálható az élővilágra veszélyes vírusok terjedése, valamint a számítógépes vírusok terjedése is.

A hálózatkutatási elmélet felhasználása azért is indokolt a kritikus információs infrastruktúrákban és ezzel együtt a döntéstámogató rendszerben, mert a különböző hálózatok hasonló tulajdonsággal rendelkeznek. Így az egyikben elért eredményeket nagy valószínűséggel alkalmazhatjuk a másikban.

A skálafüggetlen rendszerek rendkívül hibatűrőek a véletlen hibákkal szemben, de egy célzott támadás könnyen darabjaira szedheti a hálózatot, amikor a középpontokat támadják meg. Sok, kevés éllel rendelkező pont kieshet, anélkül, hogy a hálózat egészére hatással lenne. Igen fontos szerepe van a középpontoknak, amikor a vírusok, betegségek stb. terjedését vizsgáljuk. Egy középpont megfertőzése drasztikusan felgyorsítja a fertőzés terjedésének az idejét és számosságát. Az internetet tekintve a véletlen kiválasztott csomópontok 80%-ának megsemmisülése után a 20% mindig egységes hálózatot alkot. Könnyen belátható, hogy egy véletlen kiválasztott eszköz meghibásodása nem tud nagyobb zavart okozni a skálafüggetlen hálózat egészére. Kicsi a valószínűsége annak, hogy azokat a csomópontokat kapcsolom ki (hibásodnak meg),

amelyek sok kapcsolattal rendelkeznek, vagy fontosak a kapcsolattartásban. Az internetnél és a hozzá hasonló hálózatoknál a fokszámkitevő kisebb, mint három, ez a tény azt a jelenséget okozza, hogy eltűnik az a küszöb, amikor a pontok folyamatos eltávolításával egyszer csak a hálózat egésze szétesik. Hasonlóan más rendszerekhez, alkotórészeinek egy kritikus mennyiségű meghibásodása az egész rendszer összeomlásához vezethet. Különösen igaz ez a vezérlést, a felügyeletet végző információs rendszerekre. [6] [41]

Azonban a célzott támadásnál már más a helyzet. Abban az esetben, ha a csomópontokat úgy kezdjük el megsemmisíteni, hogy a legnagyobb kapcsolattal rendelkezőtől haladva megyünk a kisebbek felé, lesz egy olyan határérték, amikor a hálózat egésze szétesik. Az érdekesség az, hogy ez a kritikus pont hamar bekövetkezik, nem kell sok nagy kapcsolattal rendelkező pontot kivenni a rendszerből ehhez. Ezt azzal is magyarázhatjuk, hogy bár a rendszerünk hibatűrő, de a nagy kapcsolatokkal rendelkező pontokat (pl. központi routerek) eltávolítva igen nagy terhelést kap a többi fontos csomópont és átviteli közeg. Ezek egy ideig bírják, aztán csomagvesztések, torlódások alakulnak ki. Hasonló problémákat okoznak a fontos összeköttetéseket biztosító csomópontok is. Noha ezekhez mindig redundáns összeköttetéseket terveznek a rendszerekben, de a másodlagos már általában eleve kisebb kapacitással bír. [6]

Ezek ismeretében érdemes elgondolkodni a Spamhaus DNS-szerverei ellen végrehajtott támadáson. A DDoS[31] támadások 2013. március 18-án kezdődtek, egyes időszakokban 300 Gbps-os sávszélességet is lefoglaltak. A szerverek felé irányuló kérések átmenetileg megbénították a Spamhaus weboldalát és levelezőrendszerét. A cég kulcsszerepet játszik az internetes globális rendszerben, így az egész világra kiterjedő lassulás volt tapasztalható. A Google segítségképpen erőforrásokat bocsátott rendelkezésükre, amely enyhítette a problémát. [42]

Ebből is látszik, hogy bár az internetet általában sebezhetetlennek mondják, de ha megtaláljuk a gyenge pontjait (például hálózatelmélettel), akkor nagyon egyszerűen megtámadható, mint a hasonlóan felépített skálafüggetlen hálózatok. Az 5. ábra megmutatja, hogy a hatványfüggvény eloszlásnál kevés olyan pont van, amelynek a fokszámkitevője nagy. Ilyenek a nagyobb internetszolgáltatók routerei, webszolgáltatásokat nyújtó tárhelyei vagy a földrészeket összekötő nagyobb csomópontok. A Google azért is tudott segítséget nyújtani, mert a terheléselosztása és a

[31] DDoS (Distributed Denial of Service) – elosztott szolgáltatásmegtagadás

georedundanciája nagyon kedvező. Egy alaposan átgondolt architektúra kiépítés, egy jól átgondolt üzemeltetési szervezeti felépítés és egy jogszabályi háttér csökkentheti a gyenge pontok okozta zavart a rendszerben.

Miután megvizsgáltuk az élek változását vizsgáljuk meg a csomópontok változását is, mert az életben ezek is változnak, néha eltűnnek a csomópontok, máskor pedig megjelennek újak. Ebben az esetben már nem csak az éleket adjuk hozzá folyamatosan a hálózathoz, hanem a csomópontokat is. Folytatva a példát a gyerekek nem egyszerre érkeznek be az osztályterembe, hanem egymás után és így kezdik az ismerkedést. Barabási és Albert Réka[32] a hálózat fejlődését vizsgálva két fontos tényt rögzítettek: a növekedést és a népszerűséget.

Első lépéskén vizsgáljuk a **növekedés**t úgy, hogy tekintsünk minden pontot egyformának. Legyen két pont, majd folyamatosan adjunk hozzá egy-egy pontot a hálózathoz. Amikor egy új pont belép a rendszerbe "választ" magának két pontot, amihez éllel kapcsolódik. Már ekkor is belátható, hogy az utolsóként belépő pontoknak lesz a legkevesebb éle, az elsőknek pedig a legnagyobb az esélye a legtöbb él megszerzésére. [6]

Második lépésként vizsgáljuk a hálózatot abban a tekintetben, hogy a belépő új pontok nem véletlenszerűen döntenek az élek kiosztásáról, hanem valamilyen népszerűség alapján. Így a középpontok, amelyek népszerűbbek, mert több éllel rendelkeznek, nagyobb eséllyel kapnak újabb éleket. Egy hatványfüggvény szerint jellemezhető a hálózat. Ez a modellezés skálafüggetlen modellként vált ismerté. Összegezve elmondható, hogy a növekvő hálózatra jellemző, hogy annak a valószínűsége, hogy a belépő csomópont kapcsolódjon egy már meglévővel, arányos a meglévő csomópont fokszámával. [6] [41]

A következő lépés a hálózati modellezésben az, amikor nem csak a kezdeti fejlődést vizsgáljuk, hanem a csomópontok és élek tulajdonságainak dinamikus változását is figyelembe vesszünk. Mert egy valódi, komplex hálózatban a pontok és élek eltűnnek, erősödnek, gyengülnek, öregednek az életük során.

Természetesen nem csak a csomópontok különböznek (pl. lehetnek népszerűbbek vagy kevésbé népszerűek), hanem az éleket is súlyoznunk kell. A példánkban születnek nagyon szoros barátságok a gyerekek között és lesznek olyanok, akik a nevükön kívül nem sokat tudnak egymásról. Lesznek meghatározó egyéniségek,

[32] Albert Réka (1972-) fizikus, biológus, hálózatkutató.

akivel mindenki barátkozni akar. A hálózatba lépéstől függetlenül, azoknak az úgynevezett **centrális mutatója** nagy lesz. A hálózatelemzésben egy vizsgálati kérdés lehet, hogy az egyes csúcspontok centrális mutatója hogyan aránylik a többihez, tehát mennyi hasonló kapcsolati körrel rendelkező csomópont van a hálózatban. Másokkal viszont senki nem akar barátkozni, ők elszigetelten élik az életüket. Amennyiben fontos az is, hogy a sok kapcsolattal rendelkező személyt a többiek keresik meg barátkozási szándékkal, vagy ő akar sok emberrel megbarátkozni, akkor az irányított gráf segítségével különbség tehető közöttük. Amikor a csomópontba sok él mutat, akkor nagy **presztízzsel** rendelkező személyről (csomópontról) beszélhetünk. Amennyiben egy hálózatban túlnyomórészben kölcsönösen egymásra mutató élek vannak, akkor a hálózat **kohéziós ereje** magasnak mondható. Úgy, mint a társadalmi hálózatokban a barátságnak, az ismeretségnek is vannak szintjei, például az informatikában az összeköttetés minősége (pl. sávszélesség) sem ugyanaz két pont között. Ez lesz az egyik szempont, ami alapján egy csomóponti eszköz mérlegel, hogy a csomagokat merre továbbítsa. A **gyenge kapcsolatok** (híd kapcsolatok) éppen olyan fontosak a hálózatok tekintetében, mint az erősek. Az élővilágban a gyenge kapcsolatok biztosítják a rugalmasságot, ami biztosítja a hálózat stabilitását is. Természetesen ezek a kapcsolati mutatók változhatnak, a korábbi gyengéből lehet erős, és ennek a fordítottja is bekövetkezhet. A társadalmi hálózatokban a csoportok közötti kapcsolatokban van nagy szerepe a gyenge kapcsolatoknak. Amennyiben szeretnék egy másik, tőlem távolálló közösségbe belépni a gyenge éleken keresztül megtehetem. Granovetter[33] kutatásai szerint a gyenge kapcsolatok sokkal inkább teremtenek kapcsolatot a különböző erős kötéssel rendelkező kapcsolatok között, mint mások. [35] [43]

Véleményem szerint a kommunikációs technológia fejlődésével egyre inkább jellemzőek lesznek a gyenge kötések. A Facebook népszerűségének növekedésével például egyre több fiatal tart fenn gyenge kötésű kapcsolatokat. Ez azt is jelenti, hogy szélesebb spektrumú ismerősi kapcsolattal rendelkeznek, egyre nagyobb és bonyolultabb hálózat alakul ki. Egy adott kérdésben már nem csak a szűk ismerősi körét (erős kötéssel rendelkező kapcsolatait) keresi fel, hanem a talán soha nem látott „ismerőseit” is.

Ugyanakkor a társadalmi felépítés homofóniás volta miatt, a magasabban elhelyezkedő embereknek kisebb valószínűséggel lesznek erős kötődései, mert kisebb a

Mark Granovetter (1943-) amerikai szociológus.

merítés, kevesebb emberből tud hasonló tulajdonsággal rendelkezőt találni. A munkahelyen a vezető sem fog kialakítani szoros kapcsolatokat, a kapcsolati rendszere egyirányú lesz, vele mindenki jóban akar lenni, de ő tartja a két lepés távolságot. Kialakul a vezető magányossága. Ellenben a kapcsolati tőkéje miatt sok gyenge kötésű kapcsolattal rendelkezik, amely leginkább a beosztásának köszönhető nem pedig a személyének. Ebből következik, hogy ezek rendszerint megszakadnak, vagy tovább gyengülnek a beosztás elhagyásával. Az információ terjesztésére olyan hálózatokat kell felhasználni, amelyek sok gyenge kötéssel, hidakkal rendelkeznek, melyeket fenn kell tartani. Ennek az ellenkezője is igaz, ha nem szeretnénk az információ áramlását, illetve csak úgy, hogy az ellenőrzött formában történjen meg. A töréspontok segíthetnek a kontrolálásban, illetve az azonnali információ áramlás megszakításában. A hálózat centralista is fontos lehet a vizsgálat folyamán, mert ezeken a pontokon keresztül megsokszorozódhat az áramlás mennyisége. Ez látszólag ellent is mondhat egymásnak. A gyenge kötés a távolságot növeli meg, a szoros pedig a minél több emberhez való gyors eljutást. Azonban amennyiben nincsenek gyenge kötések, akkor nagyon hamar ugyanazt az információt többször is megkapja az egyén.

A gráfokkal történő ábrázolás hasznos lehet nagyvállalati környezetben annak szemléltetésére, hogy a végpontok, kiszolgálói központok viszonya üzemeltetéstámogatási szempontból könnyen áttekinthető legyen. A különböző nézetekkel megfigyelhetők olyan összefüggések, amelyek hálózati térképek, gráfok nélkül nem. Másik jövőbeni hasznosítása lehet a gráfoknak, hogy logikai kapcsolati rendet lehessen vázolni a hálózati infrastruktúra elemei között.

Az elméleti matematikai alapokat a későbbiekben alkalmazott matematikai módszerekkel a programozó matematikusok segítségével a hálózatelmélet és a rendszerszemlélet szem előtt tartásával ki kell fejleszteni olyan algoritmikusokat, amelyek segítségével a hálózati elemek gyenge pontjai megjeleníthetők. Más algoritmikusok pedig kedvezőbb hálózati elrendezést rajzolhatnak ki. Az értekezésemmel fel szeretném hívni a figyelmet a tudományágak keresztezésének fontosságára.

Javaslom a kormány írjon ki pályázatokat egyetemeknek a matematikai algoritmusok felkutatására és az informatikai leképzésére, továbbá a kormánya vizsgálja meg annak a lehetőségét, hogy az ország távoleső részein - figyelembe véve a felmerülő kockázati lehetőségeket is – hogyan építhetne ki stratégiai

adatcentrumokat, amelyek a nemzeti kritikus információs infrastruktúrák redundanciáját elősegítenék. A kockázatelemzésnél fel kell használni a hálózatelméleti alapokat, így elemezni kell az egyes csomópontok fokszámkitevőjét, centrális mutatóját, elérhetőségi mutatóit. Gondoskodni kell a sok kapcsolattal rendelkező és a hálózati struktúrában kulcsszerepet játszó (hídpontok) csomópontok redundanciájáról. A csomópontok és élek tulajdonságainak dinamikus változásával kapcsolatban pedig a nemzeti infrastruktúra egészét vizsgálva kell elemezni az egyes csomópontok közti sávszélességeket a hálózat kohéziós erőt. Az elemzést a A* algoritmus segítheti. Az elektromos hálózati elosztórendszerhez hasonlóan az egységes informatikai hálózat modellezésekor le lehetne játszani egy esetleges katasztrófa eseményt, ami után optimalizálni lehetne a hálózatokat. A gráfelmélet felhasználásával a személyek közti kapcsolódási pontok elemzése egy általam javasolt döntéstámogató rendszernek fontos eleme lehet, csökkenteni lehetne az emberi kockázatokból adódó veszélyeket.

2.3. MÁTRIXOK

Természetesen a gráfok önmagukban még nem dolgozhatók fel számítógéppel. Gráfokból mátrixokat kell létrehozni, amelyekkel már a számításokat el lehet végezni.

A mátrixokat úgy képezzük, hogy az oszlopok és sorok keresztmetszetében elhelyezkedő szám az élek számát jelenti. Az oszlopok és a sorok pedig a csomópontokat jelentik.

Szomszédsági mátrix

Csúcs, vagy szomszédsági mátrix segítségével adott két pont között elhelyezkedő élek számát írjuk fel. Az oszlopok és sorok keresztmetszetében elhelyezkedő szám az élek száma. Fontos, hogy a többszörös élek és a hurok élek nincsenek értelmezve A módszerrel megfigyelhető a redundancia, ami a rendszer biztonságát adja, de látható a feleslegesen sok kapcsolattal rendelkező két pont közötti összefüggés is. [11] [33] [34] [35]

a_{ij} jelöli p_i és p_j pontokat összekötő élek számát. (i sor; j oszlop)

$$\boldsymbol{A} = \left[\boldsymbol{a_{ij}}\right]$$

(3) Forrás: [11] 55. o.

Élmátrix

Az élek és csúcsok közötti kapcsolatot az élmátrix mutatja meg.

Jelölése:

$$\boldsymbol{B} = [\boldsymbol{b_{ij}}]$$

(4) Forrás: [11] 56. o.

[11] [33] [34] [35]

Elérhetőségi mátrix, Hatványmátrix

Amennyiben a szomszédság mátrixot önmagával szorozzuk meg, megkapjuk az elérhetőségi mátrixot, tehát a szomszédsági mátrix hatványa adja meg az elérhetőségi mátrixot.

Megadja, hogy a Gráf egy pontjából hány különböző úton juthatunk el egy másik pontjába. A bejárt utat a csúcspontok sorrendjének különbözősége jelenti. Ebből következik, hogy két egymás után következő pont között csak egy út lehet, hiába több él köti össze. [11]

Összegmátrix

Az elérhetőségi mátrixok összegeként megkapjuk az összegmátrixot.

Azt jelzi, hogy legfeljebb k lépésben hány egymástól független úton lehet eljutni egy adott pontból egy másik kiválasztott pontba. A gyakorlatban például a routerek forgalomirányításánál a RIP [34] egy távolságvektor alapú IGP [35] protokoll, amelyre jellemző, hogy a routing tábla tartalmazza a hoppok [36] számát. Maximum 15 router hosszúságú optimális útvonal esetén alkalmazható, mert a 16 már végtelennek számít és „megszakad” az út. [11] [13]

Szignum mátrix

Amennyiben csak arra vagyunk kíváncsiak, hogy egy adott pontból elérhető-e egy másik pont legalább egyféleképpen k lépésből, akkor a szignum mátrixot kell használni. [11]

Elérhetőségi mátrix

Amennyiben csak arra vagyunk kíváncsiak, hogy egy adott pontból elérhető-e egy másik pont akármennyi lépésből is, akkor a $Z\_(m*m)$ elérhetőségi mátrixot kell használni.

[34] RIP: Routing Information Protocol
[35] IGP: Interior Gateway Protocol
[36] Hány routeren keresztül érhető el a célállomás.

A szignum mátrix és az elérhetőségi mátrix is sokféleképpen alkalmazható az informatikai kockázatkezelés alkalmával, de a kockázatelemzéskor is vizsgálható, hogy az adott elemre lehet-e hatása egy másiknak, illetve mennyire csökken annak a hatása a kapcsolatok számának növelésével. [11] [13]

Egy csomópont kapcsolatainak a számát a **fok**kal jellemezzük. Megmutatja az i-edik elem fokát, tehát a mátrix i. sorában hány kapcsolat található.

A gráfoknál bemutatott **centralitás** számítást – tehát, hogy egy csomópont hány kapcsolattal rendelkezik – a fok centralitással számolhatjuk ki a mátrix segítségével. [44]

A Kürtös Zsófia által bemutatott számítások közül a kritikus információs infrastruktúrák vizsgálata során az egyik legérdekesebb érték a közelségi centralitás. Az adatközpont közelségi centralitása feltételezhetően a legmagasabb lesz a rendszerben, ezért fontos, hogy minden szereplő elérhesse ezt. Éppen ezért lesz érdekes megvizsgálni milyen tényezők, csomópontok helyezkednek el a köztes úton.

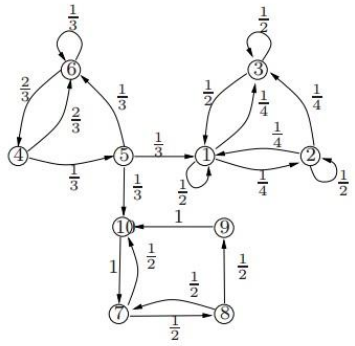
Kürtös Zsófia azonban felhívja a figyelmet arra, hogy nem mindig a legrövidebb út a legjobb választás. Figyelembe kell venni az élek súlyozását is, ami befolyásolhatja a számításunkat. Az útválasztást sokszor a sávszélesség, a megbízhatóság és még sok más egyéb tényező is befolyásolhatja, ami már az értéket torzítja. Sokszor a magas centralitással rendelkező csomópontokat választják az előbb említett súlyozások miatt a másik pont eléréséhez. [44]

A komplex hálózat megbízhatóságának elemzését a folytonos idejű, homogén Markov-folyamattal lehet elvégezni. Ez egy matematikai modellekre épülő analízis, mellyel viszonylag jól közelíthető a rendszer működése. A hálózat működését irányított és súlyozott gráfokkal modellezzük. A csomópontok az egyes állapotokat, míg az élek az állapotok közötti átmenetet írják le. A rendszer a különböző állapotokba egy sztochasztikus folyamat szerint kerülhet. μ valószínűséggel kerülhet a rendszer egyik állapotából a másikba. [44] [45]

Annak a valószínűsége, hogy a Markov-lánc *n* lépése alatt eljutok i-ből j állapotba:

$$P_{i\,j}^{(n)} = P(X_n = j | X_0 = i)$$

(5) Forrás: [46] 1. o.



$$P = \begin{bmatrix} 1/2 & 1/4 & 1/4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/4 & 1/2 & 1/4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/3 & 2/3 & 0 & 0 & 0 & 0 \\ 1/3 & 0 & 0 & 0 & 0 & 1/3 & 0 & 0 & 0 & 1/3 \\ 0 & 0 & 0 & 2/3 & 0 & 1/3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2 & 1/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

6. ábra Markov-lánc gráf reprezentációja és átmenetvalószínűség mátrixa. [46] *2. o.*

A fenti ábra egy állapotváltozást ír le, azonban más hálózati viselkedést is modellezhetnénk ezzel a módszerrel. Az ábrán az is látható, hogyan kell felírni a gráfokkal a hálózatokat, hogyan lehet mátrixba rendezni, amely már a számítógéppel is feldolgozható. A felépített modellnél lehetőség van egyszerűsítéseket végrehajtani, amely megkönnyíti a számítást. Bonyolult rendszereknél számítógépes modellezést alkalmaznak, amelyeknél különböző algoritmusokkal számolják ki a megbízhatóságot. Ilyen algoritmus pl. a Monte-Carlo módszer. [45]

2.4. ÖSSZEGZÉS

Véleményem szerint, a rendszerek bonyolultabb felépítése és a hálózatok egyre nagyobb szerkezete miatt a jövőben fontos szerepe lesz annak, hogy megismerjük a hálózati pontokat és kapcsolódásukat. A kutatásom során feldolgozott hálózatelméleti források és a szakemberekkel történő konzultáció során meggyőződtem arról, hogy a hipotézisemben (H1) feltételezett többdimenziós hálózatelméleti alapok alkalmazásának bevezetése elősegíti a rendszerszemléletű gondolkodást és új dimenziót nyit az informatikai üzemeltetés területén. Az elméleti részben bemutatott gráfok, mátrixok, párosgráfok és a többdimenziós hálózatok alkalmazása elősegítheti az üzemeltetés biztonság fejlődését. A jövőben ki kell dolgozni egy módszertant, hogyan kell elvégezni a kritikus informatikai rendszer és környezete modellezését annak érdekében, hogy az üzemeltetésbiztonság növelhető legyen.

A gráfok megrajzolása után lehetőség van az egyszerűsítésekre, valamint kimutathatók olyan összefüggések, amelyek egyébként a rendszerben nem láthatóak, de komoly zavarokat okozhatnak a rendszer egészére. Egy normál működésből igen hamar vészhelyzeti fázisba kerülhet a rendszerünk, amennyiben bonyolult, több hurkot és

felesleges redundanciát tartalmaz a rendszer. Nem biztos, hogy egy adott dolog okoz váratlan eseményt a rendszerben, amire előzetesen felkészültünk a kockázatelemzésnél, hanem sok apró, nem releváns esemény váltja ki azt. Ráadásul az én megközelítésem szerint a különböző hálózatok önállóan egydimenziónak számítanak, így beszélhetünk IT hálózatokról, emberi kapcsolatokról, infrastrukturális hálózatokról, úthálózatról, és így tovább. Azonban ezek a hálózatok nem függetlenek egymástól, kapcsolatban vannak egymással, így többdimenziós hálózatokról beszélhetünk. Egy bonyolult rendszer alakul ki így. Előfordulhat, hogy az adott hálózatban nincs kapcsolat két pont, vagy akár két szeparált IT hálózat között, de a többdimenzió miatt mégis vannak olyan élek, amelyek kapcsolatot teremtenek a két hálózat között.

Mint a többdimenziós gráfoknál írtam, egy többrétegű hálózati struktúra építhető ki az informatikai rendszerek gráfokkal történő modellezésével és így megteremthető az ember-technika-környezet kapcsolatot ábrázoló hálózati térkép. A többdimenziós hálózatok elemzésére javaslom a döntéstámogató rendszerbe beépíteni a piacon elérhető alkalmazások egyikét, amelyek akár önállóan, akár más szoftverekkel együtt alkalmazhatók.

Fontos mindenki számára tudatosítani, hogy nem nagyon léteznek független, önálló életterek, szervezetek, országok, rendszerek. A globalizáció, a technikai fejlettség miatt a mindent átszövő kapcsolatrendszereknek köszönhetően gyorsan hatnak egymásra a különböző rendszerek. Amennyiben változtatok valamit az egyik hálózatban, az nemcsak abban fejheti ki hatását, hanem láncreakcióban hatással lesz a többi rendszerben található hálózati elemekre is.

Egy skálafüggetlen hálózat nagyon stabil a véletlen hibákkal szemben, azonban mégsem alkalmas egy kritikus információs infrastruktúra létrehozására, mert a célzott támadásokkal szemben nagyon sebezhető. Törekedni kell olyan hálózat kiépítésére, ami nem a klasszikus skálafüggetlen hálózati modellt követi. Tehát terheléseloszlást kell alkalmazni az adatközpontnál, az infrastruktúráknál. A szervezeti felépítésnél törekedni kell, a hierarchiára, de nagyon fontos emellett, hogy ugyanazon feladatot egyszerre, vagy egymást helyettesítve több személy is elláthassa. Amennyiben kiesik a kulcsember legyen azonnal vele egyenértékű váltótársa. A szabályzatokkal, pontos dokumentációkkal elősegíthetjük a kieső elemek gyors cseréjét. Ezek egymással szerves egészet képeznek.

3. KRITIKUS INFORMATIKAI RENDSZER KÖRNYEZETE

Az első fejezetben a rendszer megfogalmazásakor azt állítottam, hogy a rendszerelemeket tartalmazó halmazon kívül eső részt környezetnek nevezzük. Ennek megfelelően a jogszabályokat, szabványokat és ajánlásokat éppúgy környezetnek tekintem, mint az embert, az általa alkotott szervezeti felépítést és még a folyamatokat is, amelyek befolyásolják a kritikus információs infrastruktúra (technika) működését. Ennek megfelelően vizsgálni kell annak kapcsolódási pontjait a rendszerhez. A rendszerelemek[37], hálózatok is kisebb hálózatokat alkotnak. Az egyes szabályzók, szabványok és ajánlások is összefüggésben állnak egymással – legalábbis így kellene lennie –, úgy, mint az ember alkotta közösségi hálózatok is. Ezek különböző pontokon csatlakoznak a másik hálózathoz, míg egy egész komplexebb, tulajdonságában az alhálózatoktól eltérő rendszert, hálózatot hoznak létre. Ezért is fontos minden esetben az egész rendszer vizsgálata.

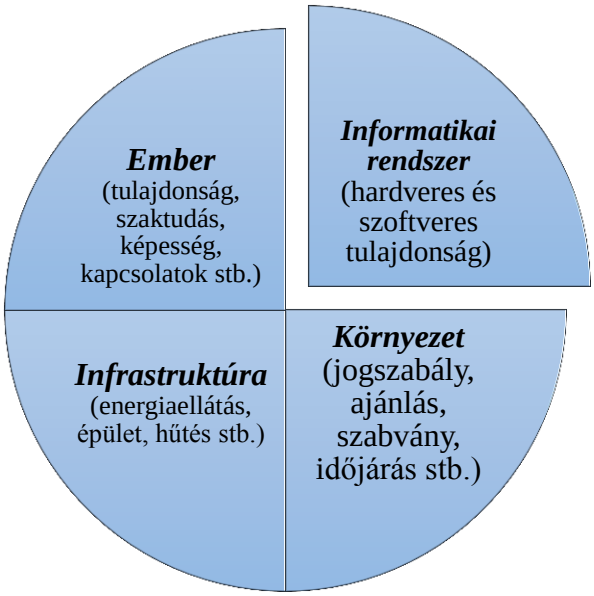
Az üzemeltetés esetében meg kell teremteni az infrastruktúra kiépítéshez és az üzemeltetéshez szükséges feltételeket, környezetet, amelyek a következők:

- pénzügyi források biztosítása (az egész életcikluson át);
- humán erőforrás biztosítása (folyamatosan jól képzett személyzet, logikusan felépített hierarchikus személyzeti struktúra);
- jogszabályi környezet megteremtése, munkafolyamatok tisztázása;
- idő (fontos a technológiai sorrend és az időtényező).

A fenti négy tényező közül a leggyengébb fogja meghatározni az egész hatékonyságát. Ezek meglétekor kialakítható egy, a célnak megfelelő technikai rendszer. A környezet, a feltételek, a hatások dinamikusan változnak. Kis mértékben az egyes elemek gyengülését korrigálhatjuk a többi elem erősítésével, a rendszer stabilitását, biztonságát azonban az egyenszilárdsággal érhetjük el.

Az általam szerkesztett 7. ábra látható, hogy a kritikus informatikai rendszerek vizsgálatakor milyen területeket kell komplex módon vizsgálni, azok hogyan befolyásolják egymást. Az ember alkotta hálózatnak kapcsolata van az IT rendszerekkel, az infrastruktúrával és a jogszabályi háttérrel, környezettel. A rendszerszemléletű gondolkodásnál az ember–technika–környezet együttes viselkedését, tulajdonságát és egymásra gyakorolt hatását kell vizsgálni. [13]

[37] Jogszabályi háttér, társadalmi rendszer, közösségi hálózat stb.



7. ábra Hálózatok összekapcsolódása
(saját szerkesztés)

A fejezetben megvizsgálom a környezetet, amelyben a kritikus infrastruktúra üzemeltetve van. Elsőként a jogszabályi hátteret, majd az ember okozta hatásokat, ezt követően a szervezetet – amely üzemelteti az informatikai rendszert –, majd a támogató tevékenységeket. [13]

3.1. AZ INFORMATIKAI TEVÉKENYSÉGET SZABÁLYZÓ FŐBB JOGSZABÁLYOK, SZABVÁNYOK ÉS AJÁNLÁSOK

A jogszabályok logikus felépítést mutatnak éppúgy, mint az általuk létrehozott szervezetek. Megtalálhatók bennük a horizontális és vertikális folyamatok, amelyek egy komplex rendszert alkotnak egymással, amennyiben minden végrehajtási rendelet kiadásra került.

Az elmúlt évtizedekben több jogszabály is született a létfontosságú rendszerekkel és létesítményekkel kapcsolatban. Szükség volt ezen szabályzók megalkotására:

- Egyrészt, mert elkezdett kialakulni egy kisebb ellentmondás abból adódóan, hogy mindenki önállóan akarta megoldani a saját informatikai rendszerének biztonságos kialakítását. A rendszerek azonban sokszor egymással együttműködnek, hatással vannak egymásra.

- Másrészt mert a kisebb vállalatok (beszállítók, kiszolgálók) és az állami szervezetek nem voltak képesek önállóan kialakítani a megfelelő üzemeltetési feltételeket. Igaz a jogszabály önmagában csak a keretet biztosítja.
- Harmadrészt szükséges volt megteremteni az összhangot más országokban létesített rendszerekkel. A létfontosságú létesítményeket sokszor bonyolult, országhatárokat is átlépő informatikai irányítórendszer vezérli, és a globalizáció hatásaként létrejött óriásvállalatok üzemeltetik. Ezért meg kellett teremteni a jogharmonizációt az országok és a különböző érdekeket képviselő szervezetek között.

2016-ban megjelent Symantec jelentésben a kiberkémkedésre, az adatszivárgásra, a lopásra hívják fel a figyelmet, amelyek a Fehérházat, a Pentagont, a Németország parlamentjének alsóházát és az amerikai kormányt is érintették. A jelentés szerint ez összesen 21,5 millió személyes adat, egészségügyi, pénzügyi, vagy újlenyomat adatot jelentett. [47]

Hipotézisem szerint (H3) azonban egy nagyos fontos részterület nincs pontosan szabályozva az informatikában, ez pedig az üzemeltetés. A rendszerek komplex intézkedési és jogszabályi kezelésével kapcsolatban már Bognár Balázs írt 2009-ben a doktori értekezésében, ahol megállapította, hogy a szabályozások nem alkotnak koherens egész rendszert, így az eltérő értelmezések károsan hathatnak a komplex védelmi rendszerre. [48] Bár nagy előrelépés történt az értekezésem megírásáig, de sajnos az üzemeltetést szabályzó rész még ma is hiányzik a komplex intézkedési és jogszabályi környezetből.

3.1.1. JOGSZABÁLYOK, KÖVETELMÉNYEK

„A törvényeknek soha nem a betűjét, hanem a szellemét kell tisztelni.”

Forrás: [49] 228. o.

Az IT biztonsági szakembereknek, rendszergazdáknak és mindenkinek, aki kritikus információs infrastruktúrával foglalkozik a törvény, a szabványok, a normák szellemiségét, a hazai és nemzetközi tapasztalatokat kell magáénak tekinteni és képviselni.

Azt hiszem az idézetet kiegészítve a következő sorokkal, amelyet Csernus Imre egyik könyvében írt a maga stílusában, teljes egészében leírja, hogyan kell kezelni ezeket a törvényeket.

„Aki tudja, hogy mit kellene tennie, de valamiért mégsem teszi, az tudatosan köpi szembe magát. Ennél jobban pedig nem alázhatja meg magát senki. Önmaga előtt."

Forrás: [50] 5. o.

A munkámból adódóan és a kutatásom során kiemelten tanulmányoztam az 1. és 2. számú mellékleteben található jogszabályokat, amelyek a kutatási témámmal is kapcsolatosak[38].

A jogi környezet kialakítása egy fontos környezeti feltétel, hogy szabályozott és biztonságos keretek között működhessenek az informatikai rendszerek. A megtett és a jövőbeni lépéseket leginkább a KRESZ [39] kialakulásának történetével lehetne összehasonlítani. A technológia fejlődik, majd elér egy bizonyos szintre, ahonnan már szabályozni kell a működést. A szabályozás először regionális szinten történt meg, majd összehangolták ezeket nemzetközi szinten is.

A kutatásom során tanulmányoztam többek között Muha Lajos és Krasznay Csaba „Az elektronikus információs rendszerek biztonságának menedzselése" című kiadványát, mely kiválóan összefoglalta az akkori jogi és szabályozási keretrendszert. [51]

A másik számomra érdekes doktori értekezés Szádeczky Tamás Szabályozott biztonság – Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertanról szólt. [52]

A két publikáció egyrészt kialakította a jogi területtel kapcsolatos gondolkodásmódomat, másrészt felkeltette bennem az érdeklődést az üzemeltetéssel összefüggő jogszabályi környezet tanulmányozásával kapcsolatban.

A feldolgozott információm szerint Magyarországon jelenleg a jogszabályok az informatikai üzemeltetéssel kapcsolatban indirekt módon három fő témakörrel foglalkoznak[40]:

---

[38] Az itt felsorolt jogszabályok és a későbbi szabványok és ajánlások listája nem tartalmazza az összes, a témával kapcsolatos anyagot.

[39] KRESZ Közúti Rendelkezések Egységes Szabályozása

[40] Természetesen vannak kapcsolódó területek is, mint például az elektronikus hírközlésről szóló 2003. évi C. törvény, de ez a három foglalkozik átfogó módon az informatikával.

- a minősített adat védelmével;
- létfontosságú rendszerek és létesítmények azonosításával, kijelölésével és védelmével[41];
- az állami és önkormányzati szervek elektronikus információbiztonságával.

Természetesen több jogszabálynak is meg kell felelni az üzemeltetés során, amely így befolyásolja azt. Ilyenek például a környezetvédelmi, egészségügyi, pénzügyi stb. jogszabályok.

Minősített adat védelme

2010. év egyfajta mérföldkő volt az információbiztonság területén Magyarországon, ezen belül is kiemelt figyelmet kapott az informatikai biztonság. Külön jogszabály szabályozza ma a minősített adatok védelmét. Míg korábban leginkább a szabványok, szokások segítették a Informatikai felső vezetőket [42] az informatikai rendszerek biztonságosabb üzemeltetésében, mára szélesebb lehetőségből választhatnak, illetve sok jogi szabályozásnak is meg kell megfelelni ezen a téren.

2009. december. 29-én került kihirdetésre a minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.). A megalkotására és minél hamarabbi bevezetésére az alábbi okok miatt is szükség volt.

1996-ban Magyarország aláírta a Nyugat-európai Unióval (a továbbiakban: NYEU) a biztonsági megállapodást, melynek értelmében kötelezettséget vállalt arra, hogy a megkapott védendő információkat az előírások szerint kezeli és tárolja. [53]

A NATO csatlakozásunk egyik kitétele volt, hogy elfogadjuk az Információ Biztonságról szóló megállapodást. Ebben rögzítették, hogy létre kell hozni egy nemzeti biztonsági hatóságot, amely az adott országban helyileg felügyeli a biztonsági feltételek meglétét. A Nemzeti Biztonsági Felügyeletről (a továbbiakban: NBF) szóló 1998. évi LXXXV. törvényt az Országgyűlés 1998. december 22-i ülésnapján fogadta el. A NBF akkor még kizárólag a NATO és NYEU Biztonsági Szabályzatában előírt követelmények érvényesítéséért volt felelős, és a polgári nemzetbiztonsági szolgálatokat irányító miniszter irányítása alatt állt. 2003-ban az EU[43]-hoz való csatlakozásunkkor a feladatköre kibővült az Európai Unió Tanácsa és az Európai Unió Bizottsága, valamint az EURATOM[44] Biztonsági Szabályzataiban leírtak érvényesítésével. [53]

---

[41] Az előző szabályozási területéhez kapcsolódik.
[42] CIO (Chief Information Officer) Informatikai felső vezető
[43] EU (European Union) Európai Unió
[44] EURATOM (European Atomic Energy Community) Európai Atomenergia Közösség

A 179/2003. Kormányrendeletben[45] a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályai már az elektronikus adatkezelésre is kitértek.

A 2073/2004. Kormány határozat[46] felhívja a figyelmet az informatikai területen való elmaradásunkra, illetve kockázati tényezőként említi az esetleges negatív következményeket.

2009-ben a Mavtv. hatálytalanította az 1998. évi LXXXV-as törvényt és előírta, hogy az azonos szintű hazai és a szövetséges adatokat ugyanolyan szintű védelemmel kell ellátni. Ezzel biztosítható az elektronikus adatok mozgatása a rendszerek között. A megfeleltetéssel egy magasabb szintre került a nemzeti adatok védelme is. A szigorítás mellett fontos előrelépés volt, hogy az informatikai rendszerek üzemeltetésével, védelmével érdemben foglalkozik a törvény és a hozzá kapcsolódó végrehajtási rendeletek. A Mavtv. megjelenését követően a 90/2010. Kormányrendelet a Nemzeti Biztonsági Felügyelet működését, valamint a minősített adat kezelésének rendjét szabályozza. Még ugyancsak 2010-ben elfogadták a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. Kormányrendeletet. [53]

A Mavtv. a minősítési szint meghatározásához az okozott kár mértékét veszi figyelembe. Így ennek alapján létezik:

- 1. „Szigorúan titkos!", amennyiben rendkívül súlyosan károsítja a minősítéssel védhető közérdeket;
- 2. „Titkos!", ami súlyosan károsítja a minősítéssel védhető közérdeket;
- 3. „Bizalmas!", ami károsítja a minősítéssel védhető közérdeket;
- 4. „Korlátozott terjesztésű!”, ami hátrányosan érinti a minősítéssel védhető közérdeket.

A rendszerekre vonatkozó fizikai, elektronikai, adminisztratív biztonsági követelményeket a 90/2010.[47] és a 161/2010.[48] Kormányrendeletekben határozták meg. A rendeletekben konkrét munkaköröket és azok feladatrendszereit is szabályozták.

[45] Hatályon kívül helyezett.
[46] A Magyar Köztársaság nemzeti biztonsági stratégiájáról.
[47] 90/2010. Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről.
[48] 161/2010. Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól.

Azonban sajnos több esetben ezeket a munkaadók a tényleges beosztás mellett elvégzendő egyéb feladatként értelmezték, értelmezik. Amennyiben ezeket a feladatokat komolyan, a törvényalkotók által elgondolt módon és minőségben látják el, akkor ez – a szervezet feladatrendszerétől, méretétől függően – egy teljes napi elfoglaltságot jelenthet. Szintén szigorú feltételeknek kell megfelelni a fizikai kiépítés esetében is, ahol a legfontosabb kategóriák a biztonsági zóna és az adminisztratív terület. A biztonsági zónán belül két osztály létezik az I. osztályú biztonsági terület, ahol a minősített adatok nyílt tárolása is lehetséges, valamint a II. osztályú biztonsági terület, ahol a minősített adatok csak zártan tárolhatók. A tárolás mellett természetesen a felhasználás is mindkét esetben megengedett. A szervertermeket, amennyiben minősített adatokat felhasználó rendszerek kiszolgálására hozták létre, tipikusan az I. osztályú biztonsági területként kell elhelyezni. A munkaállomásokat, amelyeken minősített adatokat dolgoznak fel, már lehet mindkét helyszínen használni, amennyiben az adatok tárolására alkalmas elemeit a munkavégzést követően elzárjuk egy megfelelő védelemmel ellátott helyre.

Külön kitér a jogszabály a reagáló erőkre, az elektronikus jelzőrendszerre, a beléptető rendszerekre, az ajtókra, a tárolókra, a zárakra, a falakra stb. Az újonnan épülő helyiségeket ezeknek megfelelően kell létrehozni, amelyre komoly figyelmet kell fordítani már a tervezések megkezdésekor. A tervezéseknél számolni kell a várható költségekkel, és a szükséges időtényezőkkel.

Kihívást és természetesen problémát jelent a TEMPEST követelményeknek való megfelelés is. Az elektronikai eszközök kisugárzásának leárnyékolása, elnyelése jelentősen megnöveli a kiépítés költségét és az építés során komoly odafigyelést jelent az annak történő megfelelés.

A jogharmonizáció és az említett NATO, EU tagságunk miatt az előírt követelményeket a kijelölt helyeken hazánkban is alkalmazni kell.

A Mavtv. alkalmazása amelynek egyik legkritikusabb eleleme a TEMPEST követelményeknek való megfelelés 2018. 12. 31-ig nem kötelező a törvény megjelenése előtt már üzemeltetett rendszerek esetén. A pontos megfogalmazás szerint:

„(3) Az e törvény hatálybalépésének időpontjában nemzeti minősített adatot kezelő szervnek vagy jogutódjának a nemzeti minősített adat kezelésére vonatkozó engedélyt, továbbá a nemzeti minősített adat kezelésére szolgáló elektronikus

rendszerek használatba vételére vonatkozó engedélyt 2018. december 31-éig kell beszereznie.

(4) A nemzeti minősített adat védelmére vonatkozó fizikai és elektronikus biztonsági feltételeket 2018. december 31-ig kell megteremteni"

Forrás: [19] 40. §

Ezt a dátumot az évek alatt folyamatosan kitolják a törvényalkotók.

Létfontosságú rendszerek és létesítmények azonosítása, kijelölése és védelme

Az eddigi áttekintés a minősített adat védelméről szólt, de létezik nem minősített, de védendő adat, illetve infrastruktúra, létesítmény is.

2004. júniusában az Európai Tanács egy stratégia kidolgozását kérte a létfontosságú infrastruktúrák védelméről. Ennek eredményeképpen az Európai Közösségek Bizottsága 2004. október 20-án közleményt fogadott el „A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben" címmel. [53]

Az Európai Unió Tanácsa 2005-ben határozatott hozott az információs rendszerek elleni támadásokról[49].

2005. november 17-én szintén a Bizottság egy Zöld Könyvet[50] fogadott el a létfontosságú infrastruktúrák védelmére vonatkozó európai programról, valamint döntött egy figyelmeztető információs hálózat[51] létrehozásáról. [53]

2010. november 4-én került sor az első páneurópai kibergyakorlatra. Ezt 2009-ben az Európai Bizottság közleménye tette lehetővé, amely a kritikus informatikai infrastruktúrák védelméről jelent meg „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása"[52] címmel. [53]

2010. május 19-én az Európai Unió a „Digitális Menetrend: A Bizottság akcióterve az európai jólét fellendítésére"[53] című közleményét jelentette meg. [53]

[49] A Tanács 2005/222/IB kerethatározata.
[50] COM (2005) 576 végleges.
[51] CIWIN (Critical Infrastructure Warning Information Network) létfontosságú infrastruktúrák figyelmeztető információs hálózat.
[52] COM (2009) 149
[53] IP-10-581_HU

A Digitális Menetrend célja volt, hogy létrehozzanak egy olyan rendszert, amely időben képes reagálni a számítógépes támadások ellen. Ennek keretében célként fogalmazták meg, hogy létrehozzák a CERT[54]-ek hálózatát.

Az Európai Bizottság 2010 szeptemberében két új intézkedést jelentett be, amelyek elősegítenék a védekezést Európa kulcsfontosságú informatikai rendszereit fenyegető támadásokkal szemben. Az első intézkedés az Európai Parlament és Tanács Irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat hatályon kívül helyezéséről[55]. A kerethatározat hatályon kívül helyezése mellett célja volt a kiberbűnözés elleni küzdelem megerősítése azáltal, hogy közelebb hozta a tagállamok büntetőjogi rendszereit és szorgalmazta a hatóságok együttműködését. A második intézkedés [56] az Európai Parlament és a Tanács Rendelete [57] volt, mely az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA[58]) címmel jelent meg. A rendelet célja az ENISA megerősítése, korszerűsítése és új, ötéves megbízatásának meghatározása. Az ENISA hozzájárul, hogy az EU, az EU tagállamok és az üzleti szféra szereplői szakszerűbben tudják megelőzni és kezelni a kiberbiztonsággal kapcsolatos kihívásokat. [53]

Ugyancsak 2010-ben „Az Európai Bizottság Közleménye Az Európai Parlamentnek és a Tanácsnak az EU belső biztonsági stratégiájának megvalósítása: öt lépés a biztonságosabb Európa felé”[59] címmel kiadott dokumentumával szintén célként határozta meg az informatikai hálózatok biztonságának növelését. [53]

A 3. célkitűzésben a virtuális tér biztonságának növelését határozták meg, melyet több lépésben kívántak megvalósítani.

- Kapacitásépítés a bűnüldözés és az igazságszolgáltatás terén, amely keretében számítástechnikai bűnözéssel foglalkozó központ létrehozását jelentette be, ami többek között kapcsolódási pontot jelent a nemzeti CERT-ek között.
- Együttműködés az iparral a polgárok eszközökkel való felruházása és védelme érdekében. Ebben a pontban kiemelt figyelmet kapott az

[54] CERT (Computer Emergency Response Team) – (amerikai használatban) számítógépes eseménykezelő központ, európai használatban: CSIRT (Computer Security Incident Response Team)
[55] COM (2010) 517
[56] COM (2010) 521
[57] A 460/2004/EK rendeletben döntöttek az 5 éves létrehozataláról.
[58] ENISA (European Union Agency for Network and Information Security) Európai Hálózat- és Információbiztonsági Ügynökség
[59] COM (2010) 673

információáramlás, az információkhoz való könnyebb hozzáférés. A Bizottság valós idejű központi adatbázist hoz létre a tagállamok és az ipar erőforrásainak és bevált módszereinek megosztására.

- A számítástechnikai támadások kezelésére irányuló képességek javítása. Ezt többek között a tagállamok nemzeti/kormányzati CERT-jeik összekapcsolásával kívánják elérni. A CERT-eknek hálózati elemként kell működniük egy egységes rendszerben.

Hazai tekintetben fontos rendeletnek számított a témában a 27/2004. IHM rendelet[60], amely meghatározta a kritikus infrastruktúra fogalmát.

A Kormány 1249/2010. határozatában az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról intézkedett. Eszerint kijelölte a belügyminisztert az európai kritikus infrastruktúra védelem nemzeti koordinációs feladatok végrehajtására. Továbbá egy munkacsoport létrehozására tett felhatalmazást. A munkacsoport feladataként határozta meg, hogy dolgozza ki az európai és nemzeti kritikus infrastruktúrák azonosításához szükséges kritériumrendszert. Továbbá meghatározta, hogy a lehetséges európai kritikus infrastruktúrák üzemeltetőinek vagy tulajdonosainak bevonásával tegyen javaslatot a kijelölésre és a kijelölés felülvizsgálatára. [53]

2012-ben „törvényi szintre emelkedett" a létfontosságú rendszerek és létesítmények azonosítása, kijelölése és védelmével kapcsolatos jogi háttér.[61] Az európai, nemzeti létfontosságú rendszerelem kijelölése, valamint a nemzeti és európai rendszerek kapcsolatát és közös szabályozását is tárgyalja a joganyag. A törvénynek megszületett a végrehajtási kormányrendelete.[62] A végrehajtási rendeletben pontos meghatározások vannak például arra vonatkozólag, hogy miket kell a létfontosságú rendszereknek tekinteni, milyen együttműködések szükségesek.

2013-ban elkészült Magyarország Nemzeti Kiberbiztonsági Stratégiája. A stratégia összhangban van az Európai Parlament által 2012. november 22-én elfogadott, „A kiberbiztonságról és védelemről szóló", 2012/2096(INI) számú határozat ajánlásaikhoz, továbbá a 2013. február 7-én „Az Európai Unió Kiberbiztonsági

[60] Hatályon kívül helyezett.
[61] 2012. évi CLXVI. törvény
[62] 65/2013. (III. 8.) Korm. rendelet.

Stratégiája: egy nyílt, biztonságos és megbízható kibertér" című közleménnyel. A stratégia elkészítésekor figyelembe vették a NATO 2010 novemberében elfogadott Stratégiai Koncepcióját, a 2011 júniusában elfogadott Kibervédelmi Politikáját, valamint a 2010. november 19-20-ai lisszaboni és a 2012. május 20-21-ei chicagói NATO-csúcs dokumentumaiban megfogalmazott Szövetségi kibervédelmi elveket és célokat. [53]

A Katasztrófavédelmi Koordinációs Tárcaközi Bizottság 4/2016 számú határozata alapján elfogadta az Európai hálózat- és információbiztonsági irányelv hazai jogrendbe illesztését és későbbi alkalmazásával összefüggő kibervédelmi felkészülési feladatokról szóló jelentésben foglaltakat. A 2013-ban elfogadott Európai Unió Kiberbiztonsági Stratégiájának az egyik intézkedése a hálózat- és információbiztonságnak az Európai Unión belül egységes és magas szintre történő emelésének kidolgozása volt. Az Európai Parlament és a Tanács (EU) a tagálamokkal történt hosszas egyeztetést követően a 2016/1148 Irányelvet[63] a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésről 2016. július 6-án fogadta el. Az irányelv szerint a tagálamoknak ki kell jelölni CSIRT-e(ke)t, amelyek feladata lesz az incidenskezelés és a kialakított EU CSIRT hálózat egy eleme lesz. Ennek megfelelően az Európai Unión belül (valamint szabályozza az EU-n kívüli együttműködést is) a kijelölt nemzeti illetékes hatóságoknak, kapcsolattartó pontoknak, valamint CSIRT-eknek kidolgozott együttműködési feladataik lesznek. Az irányelv továbbá bejelentési követelményeket állapít meg az alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára. Az alapvető szolgáltatásokat nyújtó szereplők körébe sorolja az energia-, a banki szolgáltatást, a közlekedést, a pénzügyi piaci infrastruktúrákat, az egészségügyet, az ivóvízellátást és -elosztást és a digitális infrastruktúrákat. A digitális szolgáltatók pedig az online piactér, az online keresőprogram és a felhőlapú számítástechnikai szolgáltatások. [54] [55]

Érdekesség és egyben megkérdőjelezi a magyar kritikus információs infrastruktúrák egységes jogi kezelését az, hogy nem minden ágazati szereplő vesz részt az együttműködésben.

„Ez az irányelv nem érinti azokat az intézkedéseket, amelyeket a tagállamok az alapvető állami funkcióik védelme, és különösen a nemzetbiztonság védelme érdekében

[63] Másképpen NIS irányelv (Directive on security of **N**etwork and **I**nformation **S**ystems)

hoznak, ideértve az olyan információk védelmét szolgáló intézkedéseket is, amelyek közlését a tagállamok ellentétesnek tartják alapvető biztonsági érdekeikkel, továbbá a közrend fenntartása, és különösen a bűncselekmények kivizsgálásának, felderítésének és büntetőeljárás alá vonásának lehetővé tétele érdekében hozott intézkedéseiket."

Forrás: [55] 1. cikk (6)

A tagállamoknak 2018. november 9-ig azonosítani kell a valamennyi ágazat és alágazati szereplőket, valamint előtte fél évvel kell a jogszabályokat megalkotni. [54] [55]

Állami és önkormányzati szervek elektronikus információbiztonsága

A harmadik szabályozott terület pedig az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.).

„Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme."

Forrás: [18] bevezető 2. bekezdés

Az elkövetkező legfőbb feladatok, amelyeket a törvény meghatároz, hogy azonosítani kell az elektronikus információvédelemért felelős személyt, meg kell határozni az adott szervezet biztonsági szintjét, kockázatelemzésre támaszkodva az elektronikus információs rendszereket biztonsági osztályba kell sorolni, valamint a meghatározott központi követelményeknek megfelelően szabályzatban rögzíteni kell a rendszerek védelmi rendszabályait. [18]

Több új gondolkodásmód is megjelenik a törvényben. Ilyen például, hogy a szervezet vezetője felelős az informatikai biztonságért, még abban az esetben is, ha annak végrehajtását egy külső cégre bízta. Kiemelt figyelmet kapott az oktatás-képzés, a kutatás-fejlesztés is.

A kiberbiztonság elérése érdekében több szervezet felállítására is felhatalmazást adnak a törvények. 2015. július 16-tól, az Ibtv. módosítással összhangban, az alábbi szervezetek léteznek ma Magyarországon:

- Nemzeti Kiberbiztonsági Koordinációs Tanács (e-közigazgatásért felelős miniszter vezeti) a Kormány javaslattevő, véleményező szerve.
- A Nemzeti Kiberbiztonsági Koordinációs Tanács munkáját a

    - kiberkoordinátor, akit az e-közigazgatásért felelős miniszter delegál;
    - valamint a kiberbiztonsági munkacsoportok, akik az egyes ágazati szakértőkből (nem kormányzati) állnak és javaslattételi joggal és véleményezési lehetőséggel rendelkeznek;
    - és a Nemzeti Kiberbiztonsági Fórum (a továbbiakban: Fórum) segíti.
- Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, melynek része
    - a Kormányzati Eseménykezelő Központot (GovCERT-Hungary);
    - a Nemzeti Elektronikus Információvédelmi Hatóság (kormányzati rendszerek);
    - a Biztonságirányítási és Sérülékenység vizsgálati terület.
- Nemzeti Biztonsági Felügyelet feladata a minősített adat védelmének hatósági felügyelete, a minősített adatok kezelésének hatósági engedélyezése és felügyelete, valamint a telephelyi iparbiztonsági hatósági feladatok ellátása.
- CERT-ek
    - GovCERT-Hungary – kormányzati eseménykezelő központ
      Feladata a kiberbiztonsági koordinációs tevékenység, együttműködés az ágazati CERT-ekkel (CSIRT-ekkel), megelőző tevékenység, incidensek észlelése, kezelése, kapcsolattartás a Hatósággal;
    - LRLIBEK[64]
      Ellátja a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenységet;
    - MIL-CERT Katonai CERT;
    - Hun-CERT az MTA SZTAKI-ban működő csoport, amely az Internet Szolgáltatók Tanácsának (ISZT) támogatásával jött létre, a nem kormányzati rendszerek tartoznak hozzá. [18]

[64] LRLIBEK Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja

Az értekezésem 3.számú mellékletében összehasonlítottam, hogy a Mavtv-t, Ibtv-t, 2012. évi CLXVI. törvényt és a 2016/1148 Irányelvet az alapján, hogy kikre (mikre) érvényesek. A 2016/1148 Irányelv magyar adaptációja még folyamatban van, de látszik, hogy bár vannak egyezések a Ibtv-ben szereplő ágazatokban, de nem minden területet található meg a másikban. Amennyiben ehhez hozzávesszük a másik két említett törvényt, akkor még több átfedés vagy éppen eltérés található. Amennyiben a törvényekhez hozzáteszem az azokhoz kapcsolódó jogszabályokat (rendeletek, utasítások stb.), az abban leírtakat, akkor az üzemeltetésben résztvevőknek nem lesz egyszerű értelmezni azokat. Főleg amiatt nehézkes a feldolgozásuk, mert a biztonságra van helyezve a hangsúly, az üzemeltetés csak ehhez kapcsolódóan található meg.

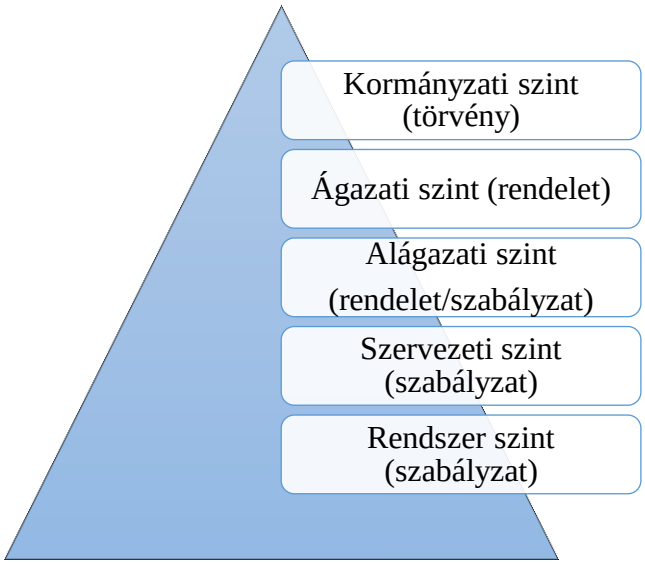
Az Európai Unión belül is vannak eltérések az ágazati besorolást illetően, de amennyiben ezt az Unión kívül is megvizsgáljuk még inkább tapasztalható. [56] A jogszabályi sokaságról pedig egy külön tanulmányt is kellene írni, mert ezek szerteágazása és értelmezése nem kis feladatot jelent az érintetek részére. [57] Azért fontos ezt a kérdéskört vizsgálni, mert a kritikus infrastruktúrák jó része nem értelmezhető csak egy országon belül, de még szervezeten (pl. NATO, EU) sem mindig. Végül pedig az egymásra gyakorolt hatásukat kellene vizsgálni, de ez sem egyszerű az előbb említett okok miatt, mert nincs egységes értelmezés. [58] [59]

A jogszabályok tanulmányozása, a szakterületen dolgozó kollégákkal történt konzultációk megerősítették a hipotézisemben megfogalmazott vélelmemet, miszerint jelenleg Magyarországon konkrétan az informatikai üzemeltetést szabályzó jogszabályi környezet hiányos. Továbbá sérül az a követelmény, hogy a szabályozások alkossanak egy koherens egész rendszert. Az üzemeltető szakembereknek egy tiszta és világos jogi hátteret kell biztosítani, amire hivatkozhatnak és később ez alapján számon is kérhetők. Természetesen, az államnak az az érdeke, hogy a kritikus infrastruktúrák stabilan működjenek, így neki kell megteremteni a feltételeket is, mint például a jogszabályban rögzített működéshez szükséges költségek. Véleményem szerint akkora mértékben kell a megrendelőnek biztosítani a feltételeket, amekkora az elvárás az üzemeltetésbiztonság irányába. Amennyiben a feltételek a megrendelő felől nem, vagy csak részben biztosítottak, úgy felmerülhet a kérdés, hogy valóban kritikus-e a működtetett infrastruktúra.

Javaslom a Magyar Országgyűlés alkosson törvényt a kritikus információsinfrastruktúra üzemeltetésével kapcsolatban, amely összhangban kell

legyen a már meglévő biztonsági kérdésekkel foglalkozó jogszabályokkal, különösképpen a Mavtv-el, a Ibtv-el, a 2012. évi CLXVI. törvénnyel, a 2016/1148 Irányelvvel és a 41/2015. BM rendelettel[65].

Meggyőződésem szerint fel kell építeni egy hierarchikus jogszabályi rendszert, amely a tevékenységek irányítását szintekre tagolná.



8. ábra Szabályozási struktúra
(saját szerkesztés)

Fentről stratégiai szinteket megfogalmazva kialakítható lenne törvényekkel, kormányrendeletekkel, miniszteri rendeletekkel stb. a kritikus informatikai rendszerek üzemeltetése. Az új jogszabályban a létfontosságú információs rendszer nagyságától és szintjétől függő szervezeti felépítésekre, munkafolyamatokra és infrastruktúra kiépítésére is ki kell térni. A szabályozás elősegítheti, hogy a létfontosságú információs rendszert üzemeltető szervezetek egységes definíciót használjanak, ezzel elősegítve az együttműködést és közös oktatási rendszer kidolgozását. A logikusan felépített jogszabályi háttérrel elérhető a stabilabb üzemeltetésbiztonság. Országos szinten egységes lenne az üzemeltetésben résztvevő személyek kötelessége és felelőssége is, ami egyértelmű képet mutatna a kritikus infrastruktúrákat üzemeltető szervezetek vezetőinek vagy más területen dolgozó személyeknek is. Az IT üzemeltetés vezetője a jogszabályokra hivatkozva megindokolhatja a döntéshozó vezetők részére, hogy az adott beruházásra miért is van szükség, még ha az egy a témában nem jártas számára

[65] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelmények.

feleslegesnek is tűnik. Ilyen beruházás lehetnek például a georedundancia[66], a mentési rendszer, a verziókövetések, a gyártói támogatások igénybevétele, a kereskedelmi szoftverek igénybevételének szükségessége, a tűzoltórendszerek, a vízbetörést jelző rendszerek stb.

Az alágazati szint és alatta lévő jogszabályok, szabályzók tartalmazzanak konkrét szabványokat[67], amelyeknek a betartásaik kötelezők legyenek.

Egyes informatikai üzemeltetési szabályzatok elkészültek, azonban ezek nem felülről szervezetten történtek, így eltérések lehetnek közöttük, nem számolnak az egymásra gyakorolt hatásokkal, nincs egységes fogalomtár, oktatás stb.

A szervezeti szinten megjelenő szabályozás tartalmazna egy BASELINE[68]-t, amelyben már részletesen szabályozva lennének az alkalmazandó módszerek, folyamatok, hardverek és szoftverek. A BASELINE akár minősített is lehetne. Az egységes kezelés előnye, hogy ezekre a rendszerelemekre lehetne kialakítani a megfelelő tudásbázist, a központi – több szintű – üzemeltető támogató háttérintézményeket.

Az üzemeltetési jogszabályokban kategorizálni kell majd a kritikus információs infrastruktúrákat aszerint, hogy mennyi felhasználó kiszolgálására alkalmasak, milyen széles spektrumot fednek le a kritikus infrastruktúra támogatásból és ami a legfontosabb, hogy a normálistól eltérő működésük, esetleges leállásuk milyen károkat okoznának. A kármérték meghatározásához minősített adatok esetében a Mavtv. 1. sz mellékletében felsorolt kategóriák, nem minősített adatok esetében a 41/2015. BM rendeletet 1. számú melléklete szerinti biztonsági osztályok képezik a szükséges kategóriákat. A besorolást elősegítheti, ha a kritikus infrastruktúrák is kategorizálva vannak. [69] Úgy gondolom nem minden ágazati, alágazati besorolás egy szinten helyezkedik el.

Amennyiben megtörténik a kategóriába sorolás, meg lehet meghatározni a jogszabályokban a hozzá kapcsolódó elvárásokat:

– az infrastrukturális[70] kiépítést;

---

[66] Georedundancia: földrajzi értelemben jól elkülönülve párhuzamosan megtalálhatóak az adatok, a feldolgozáshoz nem szükséges minden külön tárolt adat megléte, alkalmazása a biztonság vagy a gyors elérés érdekében hasznos.
[67] A következő fejezetben konkrét javaslatot teszek a szabványokra vonatkozólag.
[68] BASELINE Ebben az értelemben a konfiguráció alapállapotát jelenti, egy pillanatfelvétel, amely hivatkozási alapként szolgál.
[69] 41/2015. BM rendeletet 1. számú melléklete.
[70] adatközpont

- a rendelkezésreállás paramétereit;
- az üzemeltető szervezet felépítését;
- az éves költséget a kiépített IT infrastruktúra tükrében;
- a jogokat és a kötelességeket;
- a munkafolyamatok leírását;
- védelmi szintet,
- projektek kezelését.

3.1.2. SZABVÁNYOK, AJÁNLÁSOK

„A szabvány elismert szervezet által alkotott vagy jóváhagyott, közmegegyezéssel elfogadott olyan műszaki (technikai) dokumentum, amely tevékenységre vagy azok eredményére vonatkozik, és olyan általános és ismételten alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amelyek alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb."

Forrás: [60] 4. § (1)

Az ajánlások már egy kidolgozott, szakmai közösségek által elfogadott és jóváhagyott folyamatosan átdolgozott keretrendszert biztosítanak. Az ajánlásokra mint egy vázra ráültetve szabályrendszert hozhatunk létre, mely a saját szervezetünkre alkalmazható.

A szabvány nem minden esetben egy kötelezően betartandó utasítás. Betartása azonban erősen ajánlott, mert egyrészt a törvényben említett szakmai közösségek által kidolgozott dokumentum, így megbízhatunk benne, hogy a legmagasabb szintű tudással találkozhatunk, amivel saját szervezetünk nem minden esetben rendelkezik. Másrészről az együttműködés, beszerzések majdnem csak kizárólag így lehetségesek, mert a különböző szervezetek így egy „nyelvet" beszélnek. Harmadrészt pedig a rendszerek közötti átjárhatóság, kompatibilitás, átadási felület így biztosítható. A hátránya talán az, hogy rá vagyunk kényszerítve a globalizáció miatt is, hogy a nagyhatalmak által preferált szabványokat használjuk, amik nem minden esetben szolgálják a nemzeti érdekeket is.

Az alábbi szinteket különböztethetjük meg:

- nemzetközi szabványok
    - Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO);
    - Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission, IEC);
    - Nemzetközi Távközlési Unió (International Telecommunication Union, ITU)
- regionális szabványok
    - Európai Szabványügyi Bizottság (Comité Européen de Normalisation, CEN);
    - Európai Elektrotechnikai Szabványügyi Bizottság (Comité Européen de Normalisation Electrotechnique, CENELEC);
    - Európai Távközlési Szabványügyi Intézet (European Telecommunications Standards Institute, ETSI);
- nemzeti szabványok[71]
    - Magyar Szabványügyi Testület (MSZT);
- vállalati szabványok. [52]

Míg a szabványok használatát előírhatják nemzeti, vagy akár nemzetközi szinten is az ajánlás már nem kötelező jellegű, inkább a legjobb gyakorlatot jelenti. Az ajánlásokat lehet vegyesen alkalmazni, amellyel kialakíthatjuk a szervezetünk leghatékonyabb szabályozását.

Mint a jogszabályokat, a szabványokat és az ajánlatokat is folyamatosan nyomon kell követni, azok elavulhatnak, megjelenhetnek újabbak, vagy a frissítéseket kell alkalmazni.

Néhány informatikával foglalkozó szabvány, követelmény:

- ISO/IEC 14764-es[72] szabványa foglalja össze a szoftvertervezés és –üzemeltetés stratégiáit. [61]
- ISO/IEC/IEEE 29119 szoftverek tesztelésére létrehozott szabvány. [62]
- ISO/IEC 330xx:2015 [73] Átfogó információt nyújt a vállalatok folyamatainak méréséről, értékeléséről, minősítéséről és a

[71] A magyar szabványok megtalálhatóak a http://www.mszt.hu/ oldalon.
[72] ISO/IEC 14764:2006 - Software Engineering Software Life Cycle Processes – Maintenance

folyamatértékelés eredményeinek alkalmazásával segíti a folyamatmenedzsment munkáját. [63] [64] [65] [66] [67]

- IT4IT az Open Group által 2014-ben bevezetett szabvány, egy újfajta megközelítéssel kíván támpontot adni az IT vezetők számára, új szolgáltatások bevezetése és integrálása során. Az új szabvány csak akkor lehet sikeres, ha nem vezet be a korábbinál összetettebb, bonyolultabb eljárásrendeket. [68]
- COBIT[74] ISACA[75] által kidolgozott informatikai irányítási módszertan. *„Átfogó, nemzetközileg elfogadott keretrendszer a vállalati információ és technológia (IT) irányítására és vezetésére, amely segíti a vállalat vezetőit és vezetőségét az üzleti és kapcsolódó IT célok megfogalmazásában és elérésben."*

  Forrás: [69] 45. o.
- Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana.
- Az Informatikai Tárcaközi Bizottság 2, 3, 4, 5, 6, 7, 8, 9, 12, 13, 15, 16, 17. számú ajánlása.
- Közigazgatási Informatikai Bizottság ajánlásai.
- ITIL[76] A legfrissebb, 2011-ben bevezetett harmadik kiadásában jelent meg. Az IT szolgáltatásmenedzsment bevált gyakorlatait (best practices) összefoglaló ajánlásgyűjtemény, ami az IT üzemeltetéshez szükséges. Tehát nem szabvány, hanem a legjobb gyakorlatot mutatja be, amelyet az elméleti kidolgozást követően a tapasztalatokra építve rendeztek strukturált dokumentumba. A már kidolgozott ajánlásokat könnyebb alkalmazni a vállalatoknál és jobb az átjárhatóság a szintén hasonló ajánlásokkal dolgozók között. Az IT szolgáltatások nyújtása során szerzett tapasztalatokat összegző kiadványok öt alappillérre épülnek, amelyek a következők:

---

[73] Első rész, amely leírja a terminológiákat és a szabványcsaládot: ISO/IEC 33001:2015 ISO/IEC 33001:2015.

[74] COBIT (Control Objectives for Information and Related Technology) Vállalati információtechnológia irányításának és menedzsmentjének átfogó üzleti és vezetési keretrendszere.

[75] ISACA (Information Systems Audit and Control Association) Információs rendszerek (technológiák) auditálásával kontrollálásával foglalkozó társaság.

[76] ITIL (Information Technology Infrastructure Library) Informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan, legjobb gyakorlat.

- szolgáltatásstratégia (Service Strategy);
- szolgáltatástervezés (Service Design);
- szolgáltatás átadás (Service Transition);
- szolgáltatás üzemeltetés (Service Operation);
- állandó szolgáltatásfejlesztés (Continual Service Improvement). [20] [70] [71]

- MSZ ISO/IEC 20000-1 Informatika. Szolgáltatásirányítás. 1. rész:[77] A szabvány alapja az ITIL.

  „Az irányítási rendszer követelményeivel, a szolgáltatásirányítás tervezésével és végrehajtásával, (beleértve a változtatásokat is) a rendszerek kapacitásával, a változtatások alkalmával szükséges szolgáltatási szintekkel, a pénzügyi költségtervezéssel, az információvédelem irányításával, az üzleti kapcsolatok és a szállítók kezelésével, a váratlan események és a problémák kezelésével, továbbá a szoftverek kezelésével és elosztásával foglalkozik."

  Forrás: [72]

- Az ISO/IEC 27000-s szabványcsalád. [73]

  Az Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek követelményeit írja le.

  - MSZ ISO/IEC 27001 Az információbiztonság irányítási rendszerei. Követelmények. [74]
  - MSZ ISO/IEC 27002 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve. [75]

- ISO/IEC 27005 Információbiztonsági kockázatmenedzsment. [76]

Az EU és NATO előírásokat a szövetséges tagságunkból adódóan jellemzően adaptálni kell a magyar jogrendszerbe. A NATO szabványok azonban elsősorban a szervezetben alkalmazandó szabályokat írja le az üzemeltetéssel kapcsolatban. Az informatikai biztonsági dokumentációk terjednek ki jellemzően nemzetekre. Persze az üzemeltetés és informatikai biztonság közt itt is vannak átfedések. [77] [78] [79] [80]

Az EU, NATO szabványok mellett a német nemzeti, brit nemzeti és katonai szabványokat tanulmányoztam részletesen. **A létrehozandó nemzeti kritikus információs infrastruktúra üzemeltetéséről szóló törvény és szabályok kidolgozásakor javaslom a brit és a német szabványrendszer bedolgozását vagy**

[77] Nemzetközi változata: ISO/IEC 20000-1

ezek (pl. AJP-3.10, AJP-6 stb.) honosítását követően a betartásukat kötelezővé kell tenni. Ezek részletes iránymutatást adnak az adatközpontok kiépítésével és üzemeltetésével kapcsolatban. A brit hadsereg az újonnan kiépítendő rendszerek vonatkozásában kötelezően előírja a szabványok betartását. A 2. számú mellékletben megtalálható szabványok szinte minden részletre kitérnek, mint például rack szekrények paraméterei, berendezések rögzítése, hálózat kiépítése, külső vezetékek elhelyezése, kommunikációs infrastruktúra kiépítése és elhelyezése, kábelek kritériumai és elhelyezése, elszigetelések fizikailag, elektronikusan, logikailag és elektronikus kisugárzás tekintetében, légtechnika, hűtéstechnika, földelés, tápellátás, vészhelyzeti kikapcsolás, szigetelések, részletes leírás szerverszoba kiépítés beleértve a hőmérséklet, világítás stb., tűzoltó és jelző berendezések, tűz elleni védelem (pl. tűzálló elemek), TEMPEST, kockázatkezelés, konfiguráció kezelés, szolgáltatási szintek, adatközpont osztályozása, jelentési rendszer, BASELINE létesítése, változáskövetés, információ biztonság stb. [77] [81] [82] [83]

A nemzeti szabványosításról szóló 1995. évi XXVIII. törvény szerint a szabványok alkalmazása önkéntes alapon történik. Ezért is tartom fontosnak, hogy az üzemeltetéssel kapcsolatban a jogszabályozás megtörténjen. A fenti technikai részleteken kívül a szabályozásnak ki kell térni a szervezeti felépítésre és munkafolyamatokra, amelyet a 3.3 fejezetben részletesen tárgyalok.

3.1.3. KVÁZI SZABVÁNYOK

De facto szabványoknak nevezzük azokat a dokumentumokat:

„amelyeket általában széles körűen elismert nemzetközi civil szervezetek vagy kormányzati intézmények, szabványosítási céllal, de a szabvány formai követelményeinek teljesítése nélkül alkotnak.”

Forrás: [52] 9.o.

Kvázi szabványoknak lehet nevezni az RFC[78]-ket. Ezek olyan dokumentumok, melyeknek a célja, hogy a szabvánnyá válás előtt bárki kritikával élhet az adott anyaggal szemben. Így kialakulhat egy szakmailag megvitatott, mindenki által elfogadott szabvány, vagy elvetik és törlik a tervezetet. [78] [84]

[78] RFC (Request For Comments) kéretik megkritizálni, kvázi szabvány.

3.2. AZ EMBER OKOZTA KÖRNYEZETI HATÁSOK

A kritikus információs infrastruktúra üzemeltetéséhez elengedhetetlen a jól képzett munkaerő. Minden munkafázisban megtalálható az ember, aki a legfelső szinttől a legalacsonyabb szintig befolyásolja a rendszer működését. Ide sorolhatók a vezetők, a fejlesztők, az üzemeltetők, a beszállítók, a felhasználók, a külső tanácsadók vagy a cég más területén dolgozók, akik közvetve hatnak a rendszerre, mint a humánerőforrás gazdálkodás, pénzügy stb. Az ember, aki nélkül bármennyire is az automatizálás felé haladunk elképzelhetetlen a rendszerek üzemeltetése. Optimális esetben a rendszer közelében lévő személyek pozitív hatással vannak a rendszer működésére, azonban egyben a legveszélyesebbek is lehetnek a rendszer működésére nézve. Annyi féle természettel, háttérrel, tudással stb. rendelkező személy található meg az infrastruktúra környezetében, hogy megjósolhatatlan, milyen hatással lesznek azok működésére. Azonban a megfelelően szigorú szabályozással és kontrollal megközelíthető az optimális működési környezet. Itt is érvényes a káosz káros hatásainak a mellőzése, ebből kifolyólag irányításunk alatt kell tartani a rendszer működését, kerülni kell a véletlent, a nem várt eseményt.

Az ember negatívan kétféleképpen hathat a rendszerre, a következőek alapján.

Egyrészt akaratlanul, például nem hozzáértő módon közelítik meg a munkájukat, nem kellő odafigyeléssel végzik azt. Jellemzően ezt a problémát a belső munkatársak okozzák. Ezeket lehet szűrni, amennyiben jól képzett humánerőforrás menedzserekkel dolgozunk, akik a munkaerő kiválasztásától a folyamatos tréningeken keresztül a cégtől való eltávozásig követik a munkavállaló életútját. Természetesen pénzügyi, érdeklődés felkeltés és egyéb motivációs eszközökkel kellőképpen ösztönözhetők a magas szintű munkavégzésre a munkatársak. Emellett nagyon fontosnak tartom a szabályozási rendszer kialakítását is. A kellő gondossággal megírt szabályzók mellett az oktatást és a biztonságtudatos feladatvégzést kell elérni a munkahelyeken.

A másik negatív hatás a rendszerre, amikor ártó szándékkal teszik ezt emberek. Itt lehet külső vagy belső hatásról is szó.

Haig Zsolt és Kovács László tanulmányában találtam rá a 4. számú mellékletben megtalálható táblázatra, mely összefoglalja a külső fenyegetettségeket, amikor a szerzők a támadásokat kategorizálták. [9]

Megfigyelhető, hogy a fizikai rendszer mellett a kommunikáció, vagy a rendszer üzemeltetésében közvetlen vagy közvetett módon résztvevő személyek is támadhatók.

A legjobb módszer ezek kombinációja, kihasználva azt a jellemző hibát, hogy sok helyen a védelemmel megbízottak csak a saját területükkel foglalkoznak és egyes kisebb események talán nem haladják meg a riasztási szintet. A komplex rendszereknél azonban látható volt, hogy az alrendszerek viselkedése sokszor egészen más tulajdonsággal is bírhatnak, mint az alrendszerek összességét vizsgálva az egész rendszer működése. Emellett pedig a dominóhatást nézve egy egészen kicsi hatás is beindíthat egy láncreakciót, mely eszkalálhat egy komolyabb problémát. Mindezeket figyelembe véve megállapítható, hogy az egyes hálózatokat összegezve is vizsgálni kell, tehát az emberek alkotta hálózatot, az IT hálózatot, az energiaellátó hálózatot, az időjárást, az infrastruktúra elhelyezkedést stb.

A mai korszerű hadviselés már nem a csatamezőn történik és nem is kizárólag katonák vívják.

Porkoláb Imre egyik tanulmányában a következőket írja:

„A Határok Nélküli Hadviselés koncepciójára 1999-ben figyelt fel a nagyvilág, mivel ez a koncepció a különböző hadviselési formák integrációjának lehetőségére és a hadviselés területeinek (kibertér is) ötvözésére és ezek együttes alkalmazására tett javaslatot. Megvizsgálva a jelenlegi orosz stratégiát, úgy tűnik, hogy pontosan ennek a koncepciónak a megvalósítására törekednek. A határok nélküli hadviselés legfontosabb elemei a következők:

— mindenirányú – valamennyi terület lefedése (kibertér és űrhadviselés is), illetve a háború aspektusai széles tárházának (politikai, gazdasági, kulturális) teljes kiaknázása;

— szinkronicitás – egy időben, valamennyi területen indított műveletek alkalmazása, amelyek hatásai egymást erősítik, és integrált megközelítést tesznek lehetővé a háború formáinak stratégiai szinten történő teljes integrációjával;

— aszimmetria – bár az aszimmetria sokak szerint csak erőforrás aszimmetriát jelent, de a határok nélküli hadviselés nagy hangsúlyt fektet az információs aszimmetriai felismerésére és az információs fölény kialakítására annak érdekében, hogy a lakosságot befolyásolni tudják.”

Forrás: [85] 60-61. o.

Ez a másnéven hibrid hadviselés nagyon hatékony, már csak azért is, mert egyrészt a bizonyítható előrejelzések nagyon közel esnek a konkrét cselekményekhez, valamint a komplexitása miatt is nagyon nehéz egyértelműen meghatározni a forrást, a

célt vagy akár a támadás tényét. Oroszország jelenleg is hatékonyan alkalmazza ezt a komplex „támadási" módszert, amellyel számolni kell a kritikus információs infrastruktúrák védelme végrehajtásakor is.

A kiberhadviselés egyre szélesebbkörben történő alkalmazásásával kapcsolatban a Symantec írt éves jelentésében. 2015 december 23-án áramszünet sújtotta az Ivano-Frankivisk régiót Nyugat-Ukrajnában. Ezután, vagy inkább ezzel egyidőben több részből álló számítógépes támadás kezdődött el országszerte, melynek talán csak az volt a célja, hogy elfedje az egyéb hagyományos hadviselésből eredő tevékenységeket. [86]

Oroszország, Kína, Németország, Észak-Korea, Dél-Korea, Egyesült Királyság, Izrael, Irán stb. növelik kiberképességüket, vagy létre is hoznak egy szervezeti egységet erre a célra. Természetesen a hadsereg mellett a titkosszolgálatok is követik a trendeket. A világ államainak fel kell készülni az új kihívásokra, a rendvédelmi szervek egyikének, vagy többnek is rendelkezniük kell a kiberhadviselés képességekkel rendelkező szervezeti elemmel. Ennek megfelelően több országban még bújtatottan, de már a vezető nemzeteknél deklaráltan elkezdődött a „kiberfegyverkezés". Ennek hatására hozták létre például 2010-ben az Egyesült Államok Kibervédelmi Parancsnokságát[79]. Már korábban 2008-ban a NATO is felismerte az új terület jelentőségét, amikor felállította a Kibervédelmi Kiválósági Központot[80] Észtországban. A kibertérben történő műveletek és azok kombinálása a hagyományos hadviseléssel komoly feladatot adott a NATO részére. Hasonlóan a Genfi egyezményhez 2013-ban megalkották a Tallinni kézikönyvet[81], amely irányelvek gyűjteménye a kiberhadviseléssel kapcsolatban.

A célzott támadások azért is veszélyesek, mert a támadók legtöbbször erős szervezetek, cégek vagy akár államok, így komoly erőforrásokkal rendelkeznek a céljuk eléréséhez. A célpontnak általában nincs is információja a támadásról. Szintén nehezíti a támadás detektálását, hogy nem tudni honnan jön a támadás, ki a megbízó, ki a felderítő. A kódokat sok esetben más írja, más a támadó és más a támadásból származó eredmény haszonélvezője. A kódok többször az adott rendszerre kerülnek megírásra, kihasználva annak egyedi gyengeségeit, az üzemeltetők képességeinek hiányosságait, hibáit.

---

[79] US Cyber Command Egyesült Államok Kibervédelmi Parancsnokság
[80] Cooperative Cyber Defence Centre of Excellence Kibervédelmi Kiválósági Központot
[81] Tallinn Manual, the NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/index.html

A többdimenziós hálózatokat figyelembe véve könnyen belátható, hogy az emberi viselkedés hogyan befolyásolja közvetlen vagy közvetett módon a rendszer működését. Az előzőekben többnyire a biztonságot érintő kérdéseket mutattam be, de ezek indirekt módon az üzemeltetést is befolyásolják. Legtöbb esetben nem is kell azonban a legrosszabb dolgokra gondolni. Lehetséges, hogy az üzemeltetésbe bevont személyben az otthoni családi problémák vagy éppen örömök okoznak olyan változást, amely hatással lehet a rendszerre. Az érdektelenség, a nem kellő odafigyelés vagy a tudás, illetve tapasztalat hiánya is befolyásolhatja az informatikai rendszer üzemeltetésbiztonságát. Az utóbbi negatív hatásának kiküszöbölésére lehet megoldás a folyamatos és minőségi képzés. A rendszerbe beépített szenzorok pedig figyelhetik a megszokottól eltérő viselkedést.

3.3. SZERVEZETI FELÉPÍTÉS ÉS MUNKAFOLYAMATAI

Egy jól felépített szervezeti struktúra és a hozzá kapcsolódó folyamatok jelentősen megakadályozhatják vagy enyhíthetik az előző részben leírt emberi hibákat. A hálózatelméleti tudást felhasználva kialakítható egy olyan struktúra, amelyben a kapcsolatok előnyei kihasználhatók, a hátrányok pedig megszüntethetők vagy kontrollálhatók azáltal, hogy felfedtük őket. [56]

A 5. számú mellékletben található meg az általam javasolt nemzeti létfontosságú információs rendszer üzemeltetését végző szervezeti elemek hierarchiájának felépítése.

Javaslom, hogy a létrehozandó törvény rendelje el egy Nemzeti Létfontosságú Információs Rendszer Üzemeltetést Koordináló Testület létrehozását, amely összefogja a kritikus információs infrastruktúra üzemeltetésében résztvevő szervezeteket és együttműködik a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal. A koordináló testület feladatai közé kell tartozzon, hogy létrehozzon és karbantartson egy jogi térképet, amely eligazítja az üzemeltetésben résztvevőket (akár vizuálisan), milyen jogi környezetben kell dolgozniuk. A tanács tagjai lennének az alágazatonként kijelölt informatikai üzemeltető vezetők. A tanács elnöke egy miniszteri szintű vezető, a titkára pedig a szakmai koordinálásért felelne.

A másik fontos szervezet egy Stratégiai Kutatóintézet, amelyet szintén a törvényben kellene meghatározni. Feladata a nemzeti kritikus információs infrastruktúrák részére elméleti kutatások, hardver- és szoftverfejlesztések végzése.

A harmadik fontos terület az oktatás, amelyet szintén törvény szabályozná. Ki kell jelölni egyeteme(ke)t, amelyek specifikus képzéseket végeznének az üzemeltetők részére. A törvény ezekután előírná a szükséges képességek meglétét a beosztások ellátásához.

Végül elképzelésem szerint létre kell hozni a törvény erejénél fogva egy **központi szervezetet, amely képes lenne ellátni a** hazai kritikus információs infrastruktúrákat üzemeltetők **magas szintű szakmai támogatását**.

A szervezeti felépítésnek erősen szabályozott felépítésűnek kell lenni, amely alatt azt értem, hogy a törvényben előírt szervezeti felépítéstől és munkafolyamatoktól nem térhetnének el a szervezetek. A szervezeti egységek létszámát, előírt végzetségeket a kritikus információs infrastruktúra besorolási szintje határozná meg. A kialakított és kötelezően betartatott felépítés azért is indokolt, mert ezzel csökkenthető a gráfoknál írt skálafüggetlen hálózatok által fellépő hibalehetőségek[82]. A másik fontos oka a szabályozásnak a káosz elkerülése, aminek a veszélyéről a modellezés részben írtam. Harmadsorban pedig a felülről szerveződött hierarchikus felépítés azért indokolt, mert egyrészt a fő gazdája a rendszernek és a kockázatoknak is az állam, másrészt a központosított oktatási rendszerrel, szoftvergazdálkodással költségtakarékosabb működés érhető el. A központosítás mellett szól még a tudásbázis, az oktatás hatékonyabb felhasználása, gazdálkodása. [77] [81] [82] [83]

A létfontosságú információs rendszert üzemeltető szervezet kialakításakor az ITIL-t használtam fel. A felépítés hierarchikus rendszerű, amelyeket a következő alfejezetekben mutatok be részletesen. [20] [87]

[82] Single point of failure — egy hálózati elem gyengesége okozta meghibásodás lehetősége, ami az egész hálózat működésére hatással van.

3.3.1. FELHASZNÁLÓK KÖZVETLEN KISZOLGÁLÁSA – 1. SZINT

Ez a szint az ügyfélszolgálat által rögzített incidenskezelést, eseménykezelést, kéréskiszolgálást, változáskövetést és hozzáférés-menedzsmentet végzi. Közvetlen kapcsolatban van a felhasználókkal, ezért itt legalább olyan fontos a magas szintű ügyfélorientált gondolkodásmód és a gyors reagálás, mint a szaktudás.

Tevékenységek:

ÜGYFÉLSZOLGÁLAT – SERVICE DESK

Kapcsolódási pont a felhasználókkal, ügyfelekkel, együttműködőkkel. Fogadja a kéréseket, hibajelentéseket, rögzíti az incidenseket. Az ügyfélszolgálatot elláthatják személyesen, telefonon keresztül és virtuálisan is, amennyiben egy webes felület áll a felhasználók rendelkezésére. Az ügyfélszolgálat legtöbbször az adatrögzítésen és az előre meghatározott protokollokon kívül nem végez komolyabb informatikai munkát. [78]

INCIDENSKEZELÉS

Az incidens az üzemeltetés szempontjából egy előre nem tervezett, egyedi esemény vagy eseménysorozat, amely szolgáltatás leálláshoz, -megszakításhoz, vagy a szolgáltatás minőségének romlásához vezet. Az incidenskezelés célja a normál működés minél gyorsabb visszaállítása.

Az üzemeltetés az incidenseket hatásuk és sürgősségük alapján priorálja, elhárításukra becsült megoldási időt definiál. Az incidensek fogadására létrehozott funkció az ügyfélszolgálat, amely a kezdeti diagnózist követően, a tapasztalatok és az ismert hibák adatbázisa alapján megkísérli az incidenskezelést. Amennyiben nagyobb szakértelemmel rendelkező részlegek bevonása szükséges, az ügyfélszolgálat eszkalálja az incidenskezelést. Funkcionális eszkaláció során az egyre szűkebb szakterületre specializálódott csoportokhoz, esetleg külső vállalkozókhoz, míg hierarchikus eszkaláció során a szervezeti struktúrában magasabb pozícióban elhelyezkedő menedzserek hatáskörébe kerül át a feladat. Az incidenskezelés egyfajta kezelése lehet

egy áthidaló lehetőség választása is [83], amennyiben a további hibaelhárítást a rendelkezésre álló idő nem engedi meg. [78]

ESEMÉNYKEZELÉS

Az IT rendszerben bekövetkező változások valamilyen jelzést generálnak, amelyek tájékoztatják, figyelmeztetik a megfelelő személyt, eszközt vagy szoftvert. Azokat az eseményeket, amelyekre intézkedni kell automatikusan, vagy manuálisan valamilyen ticketing rendszerben[84] rögzítik és megkezdődhet az incidenskezelés. [78]

KÉRÉSKISZOLGÁLÁS

A felhasználóktól érkező kérések kiszolgálása történik meg. Szintén egy ticketing szoftver segítségével munkafolyamatokat szervezhetünk a kérések kiszolgálására. A kéréseket priorálhatjuk, kategorizálhatjuk, jóváhagyhatjuk, vagy éppen elutasíthatjuk.

HOZZÁFÉRÉS MENEDZSMENT

A felhasználókat (szoftvereket) az azonosításukat követően feljogosíthatjuk a szolgáltatáshoz történő hozzáféréssel. Különböző jogosultsági szinteket adhatunk a felhasználókhoz. Már a tervezési szakaszban érdemes elkészíteni a jogosultsági mátrixot a feladatkörök alapján.

Minden szinten be kell tartani a Need to Know[85] elvet. Itt egy kis ellentmondás van az üzemeltetés és a biztonsági terület között, mert az üzemeltetés hatékonyabb, ha több információval rendelkezik például egy rendszergazda [86], mint amit a konkrét feladatvégzése közvetlen igényelne.

A hozzáféréseket figyelemmel kell követni és az eseményeket tárolni kell.

[20] [73] [87] [88] [89]

---

[83] Például ideiglenes eszközzel kiválható a hibás működést okozó eszköz.

[84] Ticketing rendszer: Olyan üzemeltetést segítő rendszer, amelyben rögzíthetők a bekövetkező események, kérések és azokhoz munkafolyamatokat rendelhetünk.

[85] Mindenki csak a szükséges információt ismerje meg, ami a munkájához közvetlen, vagy közvetett módon kapcsolódik.

[86] Rendszergazda alatt az értekezésben a rendszeradminisztrátort értem.

3.3.2. IT RENDSZEREK ÜZEMELTETÉSE – 2. SZINT

Ezen a szinten közvetlen már nincs kapcsolat a felhasználókkal. Célszerű a tevékenységet két részre bontani:

- Rendszer üzemeltetés: szerverek, adattárolók, adatbázisok, archiváló és mentőrendszerek telepítése, konfigurálása, üzemeltetése, felügyelete, karbantartása.
- Telekommunikációs, hálózati rendszerek üzemeltetése: hálózati infrastruktúrák (router, switch, tűzfalak, modem, kábelek) konfigurálása, üzemeltetése, felügyelete.

KARBANTARTÁS

Elengedhetetlen egy infrastruktúra jó megtervezése és folyamatos karbantartása, amely hozzájárul az üzemfolytonossághoz. Ennek az elemnek a sérülése komoly, sokszor visszafordíthatatlan katasztrófákhoz vezethet az egész rendszerben.

Számos karbantartási stratégia létezik, azonban a kritikus információs infrastruktúra esetében gondosan kell megválasztani melyiket alkalmazzuk. a következő felsorolás közül:

- Hibaelhárító[87] karbantartás esetén a rendszer minden esetben a meghibásodásig üzemel, így a javítás előre nem tervezhető és esetenként túl hosszú időt vehet igénybe. A váratlan leállások miatt ezt nem alkalmazhatjuk. [70]
- A tervszerű megelőző karbantartás[88] számol a meghibásodások várható idejével. Előnye, hogy a karbantartás tervezhető, azonban az előzővel ellentétben már akkor is munkavégzéssel jár, ha nem szükségszerű a munka. [70]
- Az elvégzett munka szerinti fenntartás[89] nem előre rögzített, hanem az adott rendszerelemek egyedi, jellemző paraméterei (pl.: üzemidő, futásteljesítmény) alapján határozza meg a karbantartási periódusokat. Tervezhető és gazdaságosabb az előzőnél. [70]
- Állapotfüggő karbantartási stratégia[90] az előző továbbfejlesztett változata, itt már nem csak a paraméterek adatait veszik figyelembe, hanem időszakosan vagy

[87] FBCM (Failure Based Corrective Maintenance) Hibaelhárító karbantartás
[88] PM (Preventive / Planned Maintenance) Megelőző karbantartás
[89] PCBM (Parameter Condition Based Maintenance) Paraméter kondíció szerinti karbantartás
[90] CBM (Condition Based Maintenance) Állapotfüggő karbantartás

folyamatosan is mérik azok jellemzőit. A valószínűségszámítást és statisztikát felhasználva ezen adatok alapján tervezhető a karbantartás ideje és minősége. [70]

- A megelőző, vagy proaktív karbantartás [91] a tervezési hibákkal is számol, amelyet a bekövetkező vagy várható meghibásodások mellett megelőző javítással előz meg. [70]
- A megbízhatóság központú karbantartási stratégia [92] a korábbi stratégiák keveréke, az állapotjellemző paraméterek és a várható karbantartási periódusok alapján értékelik a rendszer megbízhatóságát. Amennyiben ez az érték egy küszöbérték alá esik, elvégzik a karbantartást. [70]
- A teljes körű hatékony karbantartás[93] módszere az üzemeltetési folyamatokba a fejlesztőket és a felhasználókat is bevonja. [70]
- A kockázat alapú stratégia a meghibásodási valószínűségek és a lehetséges következmények értékelésével határozza meg a karbantartás idejét. Az állapotfüggő karbantartással együtt alkalmazva hatékony módszer dolgozható ki, amely növeli a rendszerelemek rendelkezésre állását, előre meghatározott kockázati szint mellett minimalizálja a karbantartásra fordítandó összeget és gyors információáramlást biztosít az üzemeltetési tevékenység biztosításához. [70] [90]

3.3.3. HÁTTÉRTÁMOGATÁS – 3. SZINT

Feladatuk:

- a fenti két szinten időben meg nem oldott incidensek kezelése;
- a problémakezelés;
- az informatikai rendszerek üzemeltetéséhez magas szintű tudás hozzáadása;
- kezelési, telepítési és konfigurációs dokumentumok elkészítése, karbantartása.

A problémakezelés során a cél az incidensek ismeretlen okainak feltárása, azok dokumentált rögzítése. Az incidenskezelés a gyors megoldást helyezi előtérbe, abból a célból, hogy a szolgáltatás minél előbb helyreálljon, míg a problémakezelés a megelőzést is magába foglalja, a hibák okát vizsgálja, annak érdekében, hogy azok ne

[91] Proactive Maintenance Megelőző karbantartás
[92] RCM (Reliability Centered Maintenance) Megbízhatóság központú karbantartás
[93] TPM (Total Productive Maintenance) teljes körű hatékony karbantartás

ismétlődjenek meg, illetve soha ne is következzenek be. A kategorizálás és priorizálás itt is megtörténhet, de az incidenskezelésnél meghatározott prioritása eltérhet a problémakezelésnél levőtől.

Amennyiben nem oldható meg viszonylag rövid időn belül a hibaelhárítás, akkor át kell adni egy kijelölt és felkészített magasabb szintű hibaelhárító csapatnak, ami ebben az esetben már külső szolgáltató, vagy gyári támogatás. [20] [88] [89]

A felügyeleti és beavatkozó rendszernek rendelkeznie kell olyan tudásbázissal, amely segít feldolgozni a későbbi problémákat, illetve összekötve a változáskövetéssel és a nyilvántartó rendszerrel, elemzéseket képes lefuttatni, ahol a hálózatelméleti alapok tudnak segítséget nyújtani. [91]

3.3.4. ELEKRTONIKUS INFORMÁCIÓBIZTONSÁGI CSOPORT

Az információbiztonsággal kapcsolatos konfigurációk meghatározása, IT védelmi szoftverek konfigurálása, üzemeltetése, felügyelete a csoport[94] feladata. A rendszerelemek esetében (szerver, router, adattároló stb.) olvasási jogokkal rendelkeznek, ezek konfigurációját az IT rendszereket üzemeltető állomány végzi. Hálózatelméleti szempontból fontos az előbbiek szétválasztása. Egyrészt az üzemeltető állomány rendelkezik a kellő szakértelemmel, másrészt ők látják át a rendszer egészét konfigurációs szempontból[95], tehát ismerik a hálózati csomópontokat és éleket. Az informatikai biztonsági cél a beállítások során többféleképpen elérhető, egy hibás konfiguráció azonban nem kívánt hatást fejthet ki a hálózat egy más csomópontjára, vagy a rendszer egészére. [91] [92]

Az információbiztonság szempontjából mindennapos gyakorlatnak tekinthető intézkedések közé tartoznak az alábbiak:

- kockázatfelmérés és kockázatjavítás;
- az információbiztonsági politika dokumentuma;
- az információbiztonság szervezete;
- emberi erőforrások biztonsága;
- fizikai és környezeti biztonság;
- hozzáférésellenőrzés;
- az információbiztonsági incidensek kezelése;

[94] Mérete változó akár egy fő a szervezet és az informatikai rendszer felépítésétől függően.
[95] Teljesen más szemszögből kell nézni a rendszerre a két területnek.

- információbiztonság tudatosság, képzések szervezése;

működésfolytonosság irányítása. [74]

A szervezetünkre kidolgozott informatikai biztonsági dokumentumban megfogalmazott irányelveket a szervezet minden tagjának be kell tartani és a szükséges technikai dokumentumoknak (konfiguráció, telepítés stb.) összhangban kell lenni ezekkel.

3.3.5. KISZOLGÁLÓ INFRASTRUKTÚRA ÜZEMELTETÉS

Az adatközpont kiszolgáló eszközeinek üzemeltetése. Ilyen lehet a riasztó, beléptető rendszerek, tűzjelző, vízbetörésjelző, zártláncú kamerarendszerek, UPS, aggregátor, légtechnikai eszközök technikai üzemeltetése, karbantartása. Ezeket jellemzően különálló szervezeti elemek végzik, azonban szükségesnek tartom ezen elemek ki és bemeneti információit összekötni a kiépítendő felügyeleti és beavatkozó rendszerbe.

3.4. ÜZEMELTETÉST TÁMOGATÓ TEVÉKENYSÉGEK

3.4.1. PÉNZÜGYI ERŐFORRÁS

A pénzügyi és számviteli munkák mellett folyamatosan biztosítani kell a szolgáltatás bevezetésének, üzemeltetésének és kivezetésének a költségét.

Az IT sikeres működtetésének egyik legfontosabb feltétele a folyamatos és szükséges pénzügyi források biztosítása. Ennek érdekében el kell készíteni a rövid és hosszú távú pénzügyi terveket. A tervezést támogathatja a konfigurációs adatbázis, amelyben pl. az eszközök gyártói támogatásának a lejárata, vagy a tervezett cseréje van nyilvántartva, így pontosan tudható azok várható kivezetésének ideje.

Általában az informatikai költségekre a vezetők egy számukra megfoghatatlan, értelmezhetetlen kiadásként tekintenek, mivel sok olyan elemet tartalmaznak – szerverek, hálózati eszközök, levelező rendszerek, adattároló rendszer, mentő rendszerek, biztonsági rendszerek, és ezekhez tartozó szoftverek stb. amelyek el vannak rejtve a felhasználók elől, közvetlenül nem, vagy csak közvetve találkoznak velük. Meg kell határozni a önköltséget[96], a rendszerünk tervezhetősége érdekében és ezzel

[96] Önköltség Total cost of ownership

számolni kell az éves költségvetési tervben is. Mind a nemzetközi, mind a hazai tapasztalatok szerint az informatikai rendszerek megfelelő szinten történő működtetése érdekében az IT szektorra jutó költségeknek el kell érnie az összköltségvetés legalább 2 százalékát. Az ideális pedig a 4-5 százalék, amellyel ki lehet szolgálni az üzemeltetéssel járó mindennemű igényeket. [93]

3.4.2. TUDÁSMENEDZSMENT

A szolgáltatásbiztosítás különböző fázisaiban összegyűlt információt, tudást, tapasztalatot és adatot egy visszakereshető formában kell tárolni. Az adatbázisban történő tárolás lehetővé teszi az elemzéseket és az összefüggések keresését, amely a jövőre nézve komoly előnyökkel járhat. A CMS-re építve a jelenben és a múltban történt események, változások és a felhalmozott tudásbázis nagyban elősegíti a döntéshozatalt egy adott kérdésben. Ez lesz a szolgáltatás tudásmenedzsment rendszer.[97] [20]

Az üzemeltető személyzetnek folyamatos képzéseken kell részt venniük, annak érdekében, hogy a rendszerhez szükséges naprakész tudással rendelkezzenek.

3.4.3. RENDSZERTÁMOGATÁS

Amennyiben a 3. szintű üzemeltetői támogatás sem képes megoldani a keletkezett problémát vagy a rendszer fejlesztésére van szükség, igénybe kell venni a rendszertámogatást. Ezt egy szerződött, szervezeten kívüli cég végzi. A rendszerházak, erre szakosodott rendszerintegrátorok tapasztalt, jól képzett szakemberekből állnak, akik egy bizonyos területen nagyon mély ismeretekkel rendelkeznek. A speciális ismereteket egyetlen szervezet sem tudná gazdaságosan kihasználni, mivel folyamatosan ilyen mélységű tudásra nincs szüksége a napi üzemeltetés területén. A külső rendszerintegrátorok üzleti és informatikai tanácsadással, rendszerek tervezésével, bevezetésével foglalkoznak. A javasolt jogszabály létrehozásakor ezt a szervezetet kellene létrehozni államnak.

A legmagasabb támogatást akár a hardver- vagy szoftvergyártók is nyújthatják. „Alvó szerződéseket" kell kötni, amelyek kizárólag egyedi esetekben (katasztrófahelyzetekben, problémakezelésnél, rendszerfejlesztésnél) lehet aktivizálni.

---

[97] SKMS (Service Knowledge Management System (Szolgáltatás) Tudásmenedzsment Rendszer

3.4.4. INFRASTRUKTÚRA FENNTARTÁS

A kritikus információs infrastruktúrákat kiszolgáló épületek felépítése és üzemeltetése során keletkezhetnek olyan információk, amelyek az informatikai rendszer üzemeltetés szempontjából fontosak lehetnek és ez igaz fordítva is. Ezekkel az adatokkal számolni kell az üzemeltetés folyamán.

3.4.5. MEGFELELŐSÉG, AUDITÁLÁS

A szervezetet és a rendszert auditálni kell, annak érdekében, hogy egy független szervezet is kimondja, hogy a szabályok és belső folyamatok megfelelnek az előírt követelményeknek. Ezt a tevékenységet mindenképpen a szervezetünktől független szakértői cégre szükséges bízni, akik elfogulatlan értékelést tudnak adni a szervezetünkről és a rendszerünkről. A rendszer üzemeltetése során törekedni kell arra, hogy megfeleljünk minden törvényi és szabályozási előírásnak, betartsunk minden szerződésben foglalt kötelezettséget, a szellemi tulajdonjogokat, a személyes adatok bizalmasságát és az adatok védelmét. Az auditálásban segítséget nyújthat a felügyeleti rendszer, amely tartalmazza azokat a template-ket[98], amelyekre szükség lehet a beállítások során. [74] [94]

3.5. ÖSSZEGZÉS

A kialakított üzemeltetési és védelmi struktúrában minden személynek, eszköznek megvan a szerepe, felelőssége. Tisztázva vannak a kommunikációs csatornák, a vertikális és horizontális együttműködések. Együttműködést kell biztosítani a biztonsági területen belül dolgozókkal (a cégen belül a munkavédelemmel, egészségvédelemmel, tűzvédelemmel stb.), az IT szakemberekkel, a külső cégekkel. A sikeresség csak egy központosított irányítási rendszerrel érhető el, amelynek része az egységes és homogén informatikai rendszer. A fejezetben leírtaknak alapján a hipotézisemben (H2) megfogalmazott állítás helyességében megbizonyosodtam. Eszerint amennyiben sikeresen akarjuk üzemeltetni az informatikai rendszerünket egy szigorúan szabályozott struktúrát kell kiépíteni, mind a szervezeti felépítésben, mind a környezeti jogszabályok területén és az informatikai rendszerünket kiszolgáló

[98] Olyan dokumentum vagy script, amelyet korábban teszteléssel igazoltak, hogy az abban szereplő beállításokkal a rendszerünk a kívánt állapotba kerül.

infrastruktúrában is [99]. Ezzel elkerülhető a fejezetben leírt káosz kialakulása és enyhíthető az értekezésben megfogalmazott emberi mulasztásokból vagy szándékosan okozott károk hatásai. Továbbá amennyiben a rendszerszintű felépítésünk egy egészet alkot, akkor oktatási rendszert is építhetünk mögé. A kritikus információs infrastruktúra üzemeltetése üzembiztosabbá tehető, amely átlátható és megbízható környezetet biztosítana a területen dolgozók számára.

Az értekezésemben rámutattam a területet jellemző jogszabályi hiányosságokra, a rendszerszintű gondolkodás fontosságára. Az üzemeltető vezetők általában a saját maguk által létrehozott üzemeltetési és egyéb utasításból dolgoznak. Sajnos még az informatikai szakemberek körében sincs mindig mindenben egyetértés az üzemeltetés során.

A fejezetben megfogalmazott jogi környezet hiányosságait feltárva, a hipotézisemben (H3) állítottak helytállóak voltak, mert ma Magyarországon az állami szektorban üzemeltetett kritikus informatikai rendszerek üzemeltetéséhez szükséges jogszabályi hátterek valóban hiányosak. A szabályozói környezet hiányosságának kiküszöbölése, mind az üzemeltető személyzet, mind a felügyeletet ellátók érdekében szükséges. A jogszabályoknak rendelkeznie kell a kritikus információs infrastruktúra kiépítési kritériumáról. A fejezetben bemutatott szervezeti felépítés, támogató tevékenységek mind része kell legyen a szabályozásnak.

Létre kell hozni egy a már meglévő informatikai biztonsági jogszabályokkal összhangban lévő informatikai üzemeltetést támogató jogi környezetet, amelyek egy koherens egészet alkotnak. A BASELINE-ban szerepeltetni kell a legfelső szinttel a végrehajtási utasításokkal összhangban lévő módszereket, folyamatokat, hardvereket, szoftvereket. Ezek ágazatonként lehetnek eltérőek is, de biztosítani kell a közöttük lévő összhangot.

Végül pedig problémának látom, hogy Magyarországon jelenleg olyan sok a kijelölt (vagy kijelölendő) kritikus infrastruktúra, hogy már a kritikusság szót veszélyezteti a mennyiségük. Ennyi területre képtelenség koncentrálni, biztosítani a pénzügyi és egyéb erőforrásokat. Ezeket az ágazatokat, alágazatokat és magukat a létesítményeket központilag kategorizálni, súlyozni kell. A 41/2015. BM rendeletet előírja a kategorizálást, de ezt felülről szerveződve kell megtenni az országban található összes kritikus információs infrastruktúra esetén.

[99] Részletes leírást erre vonatkozólag a következő fejezetben található.

A komplex szabályozottság abban mutatkozik, hogy az egyes rétegek közötti kölcsönhatás[100] eredményeképpen a teljes rendszer egy minőségileg új, az egyes részektől eltérő viselkedést mutat. Emiatt is félrevezető az a tévesen kialakult gyakorlat, hogy az egyes kritikus információs infrastruktúrát üzemeltető szakemberek nem gondolkoznak komplex rendszerekben, így a rendszerelemek vizsgálatakor téves kép, téves biztonságérzet alakul ki bennük.

A következő fejezetben leírtak a döntéstámogató rendszer kritériumainak meghatározása mellett szintén fontos információt[101] tartalmaznak a jogi szabályozás szempontjából.

[100] Többdimenziós hálózatok közti kapcsolat.
[101] Érettségi szintek, állapotváltozások, Adatközpont kialakítása.

4. KRIRIKUS INFORMÁCIÓS INFRASTRUKTÚRA ÜZEMELTETÉSE

Eddig tisztáztam, hogy a logikusan felépített rendszer üzemeltetésének szervezetszerű irányítás és kontroll alatt kell állnia. A hierarchikus felépítés és a rendszerszemléletű gondolkodásmód elengedhetetlen egy kritikus információs infrastruktúra üzemeltetésénél, amitől eltérő felépítés a rendszerben váratlan, nehezen kezelhető hibákat eredményezhet. A fejezetben az üzemeltetés esetében fontos építőelemeket elemzem – majd hipotézisem szerint (H4) – bemutatva, hogy ezen építőelemek felhasználásával kell létrehozni egy üzemeltetést segítő döntéstámogató alkalmazást (felügyeleti és beavatkozó rendszert), amely egy CMS kibővített változata és a kockázatkezelő modul szerves része.

A fejezetben a kutatásom alatt összegyűjtött infrastruktúrával kapcsolatos információkat rendszerezem, annak érdekében, hogy alátámasszam mennyire fontos része a kritikus informatikai rendszerek biztonságos üzemeltetése szempontjából az infrastrukturális háttér. A felügyeleti és beavatkozó rendszer kiépítésének alapfeltétele, hogy ismertek legyenek annak építőkockái, így megvizsgáltam a kritikus informatikai rendszerre jellemző érettségi szinteket, állapotváltozásokat, az adatközpont elemeit, jellemzőit. Ezen tulajdonságok mellett még fontos a kockázatelemzés megismerése, amelyet szintén ebben a fejezetben fejtek ki.

4.1. ÉRETTSÉGI SZINTEK

Függetlenül attól, hogy új kritikus információs infrastruktúrát kell építeni, vagy az üzemeltetett régit kell továbbfejleszteni, célszerű lépésenként előrehaladni. Ennek érdekében meg kell ismerni a rendszerre jellemző érettségi szintet. A COBIT szabványban leírtakat felhasználva[102] értékelhető a rendszert aszerint, hogy az éppen milyen érettségi szinten van az üzemeltetés szempontjából. A jelenlegi állapot és az elérendő cél függvényében cselekvési tervet kell készíteni, amelynek alkalmazkodnia kell a cég stratégiai elképzeléseihez. Számomra azért érdekes ez a kérdés, mert az általam javasolt felügyeleti rendszer csak a 4. szinttől vezethető be. A teljesség igénye nélkül kiemelek néhány jellemzőt, amely az általános és a szolgáltatás folytonosság modellben található [95]:

[102] Az ISO/IEC 330xx szabványcsalád szintén a folyamatszabályzás, értékelést és osztályozást írja le. Átfogó információt nyújt a folyamatértékelés fogalmáról, a folyamatminősítés alkalmazásáról. [63]

0 Nem létező — Ennél a szintnél a vezetésnek tudomása sincs arról, hogy tennie kellene valamit. Nincsenek is szervezett folyamatok, amelyek elősegítenék a rendszerszintű működést. [96]

1 Kezdeti/Ad Hoc jellegű — Egy-egy estben már vannak olyan ideiglenes folyamatok, amelyek elősegítik az informatikai üzemeltetést. Ezek viszont csak egy két területre, vagy időben behatároltan léteznek. Előnye, hogy a vezetés felismerte, hogy kezelni kell bizonyos eseteket, azonban ez sem dokumentálva nincs, sem pedig eljárásrendek sincsenek. A felelősségek és jogosultsági kérdések nincsenek egyértelműen megfogalmazva. A vezetési és irányítási módszerekben nem fedezhető fel rendszer. Az esetleges hibákra, incidensekre jelentős késéssel reagálnak. [96] [97]

2 Ismétlődő, de ösztönös — A munkafolyamatok már szervezettetek abból a szempontból, hogy ha már találkoztak hasonló problémával az üzemeltetők, akkor konkrét cselekvési tervek vannak. Ezek azonban nincsennek formalizálva, dokumentálva és ebből adódóan nincs rá oktatás szervezve és nem is számonkérhetők. Ez a szint már megkívánhat adatbázisokat, amely a későbbiekben alapja lehet az általam javasolt a rendszernek, azonban ezek az adatok még megbízhatatlanok.

Hátránya, hogy az üzemeltetők tevékenységei még nincsenek összehangolva, így ki-ki a saját maga tudása és képessége szerint végzi a feladatát. A rendszerbe bele vannak kódolva az egyéni hibák. [96] [97]

3 Szabályozott folyamat — Ezen a szinten a munkafolyamatok már egyértelműen rögzítve vannak, így biztosítva van, hogy rendszerszerű megoldások szülessenek egy kialakult problémára vagy egy munkafolyamatra. Annak érdekében, hogy mindenki elsajátítsa az ismeretanyagot és egységes munkavégzés történjen már vannak oktatások. Ezen a szinten már azonosíthatók a javaslatomban is szereplő szabályozott munkafolyamat és strukturális szervezeti felépítés kezdeti jelei. Azonban a kialakult eseményekre még csak tapasztalati úton vagy egyéni megoldásjavaslatokon született válaszreakciók vannak formalizálva. Egy-egy terület felelősei és döntéshozói már ki vannak jelölve. Fellelhető az „üzemeltető szervezet felépítése és munkafolyamatai” részben leírt szervezeti bontások. Technikai oldalról már léteznek a magas rendelkezésreállást elősegítő redundanciák. A munkafolyamatokat támogató adatbázisok ezen a szinten már megbízhatóak, így építeni lehet rájuk. [96] [97]

4 Irányított és mérhető — A folyamatok eredményességét a vezetők rendszeresen figyelik, mérik és a nemkívánt hatások megszüntetésére intézkedéseket

tesznek. Annak érdekében, hogy a folyamatok már ne függjenek a cégben dolgozók tudásától a szabványosított munkafolyamatokat már különböző jól bevált gyakorlatokra építik. Ezen a szinten való gondolkodással már eredményesen alkalmazható a jogszabályokat leíró fejezetben lévő javaslataim.[103] A megoldásokban csak elvétve találhatók automatizmusra épülő folyamatok. Az incidenseket és problémákat priorizálják és mindenki számára egyértelmű a folyamat az egyes eseményekre. A rendszerben szigorú szabályok szerint történik a jóváhagyási mechanizmus. [96] [97]

5 Optimalizált — A kialakult eseményeket gyorsan lekezelik, köszönhetően a gyakori automatizmuson alapuló folyamatoknak is, valamint a szabályozott strukturális felépítésnek és munkafolyamatoknak. A munkafolyamatokat eszközök és szoftverek segítik elő, amelyek auditálva vannak. Az informatikai üzemeltetési szabályzatok teljesen összhangban vannak a cég üzleti működésfolytonossági tervében leírtakkal, amelyeket rendszeresen karbantartanak. A vezetés kiemelten kezeli, hogy a kritikus információs infrastruktúra működési feltételei minden irányból biztosítva legyenek. [96] [97]

Nyílvánvaló, hogy a cél egy kritikus információs infrastruktúra esetében, hogy a rendszerünk mindig az optimatizált szinten működjön. Sajnos tapasztalatom és az információ gyűjtés alapján azt a következtetést tudom levonni, hogy ma Magyarországon a legtöbb rendszer nem közelíti meg az üzemeltetés szempontjából az optimális 5. szintet. Ennek oka többrétü. Egyrészt pénzügyi okai vannak, de esetenként a terület szabályozatlansága, a szakemberek helytelen gondolkodása, valamint a vezetői elkötelezettség hiánya (ami sokszor az információhiányra vezethető vissza) okozza az alacsony szintre történő besorolást.

A szintek meghatározása nem azonos a 41/2015. BM rendeletben megfogalmazott biztonsági szintbe vagy biztonsági osztályba sorolással. A fenti érettségi szintek kizárólag az üzemeltetési szempontból értelmezhetőek.

4.2. ÁLLAPOTVÁLTOZÁSOK

Az kritikus információs infrastruktúrára épülő döntéstámogató rendszer kiépítését a villamosenergia átviteli rendszerirányítást tanulmányozva képzelem el megvalósítani. A vezérlő a működése során 7 állapotot kezelhet. [98] [99]

[103] ARPA (Advanced Research Projects Agency) Fejlett Kutatási Projektek Ügynöksége
[103] Paul Baran (1926-2011) lengyel születésű, amerikai mérnök

Tervezési fázis

Már a létfontosságú rendszerelem tervezésekor megkezdődhet a kockázatelemzés, amikor betáplálhatjuk a kezdeti értékeket, modellezhetjük a döntéstámogató rendszer működését és javíthatunk a végleges megvalósítási terveken. A szoftvert hozzáigazíthatjuk a környezethez, modelleket alkothatunk a rendszerről, megtervezhetjük a szenzorok elhelyezését, optimalizálhatjuk a bemenő adatok mennyiségét. [98] [99]

Beállási fázis:

A már megépített kritikus információs infrastruktúrához hozzáigazítjuk az alkalmazást. A felügyeleti rendszer szempontjából ez egy kezdeti tanuló állapot, amikor a sok elsődleges adatból adatbázist építünk, az adatkapcsolatokból a mesterséges intelligencia segítségével tanítjuk a rendszert. [98] [99]

Normál üzemállapot:

A létfontosságú rendszerelem normál üzemben dolgozik, a szoftver nem érzékel semmi, a normálistól, elvárt állapottól eltérőt. Nem észlelhető olyan állapot, amely az előzetes kockázatelemzéskor felmerült. A szenzorok folyamatosan szolgáltatnak adatot a kockázatelemzéshez (dinamikus kockázatelemzés). [98] [99]

Készültségi állapot:

A döntéstámogató rendszer az előzetesen azonosított kisebb kockázati tényezőt érzékel, de ez nem befolyásolja a kritikus információs infrastruktúrát a működésében. A kockázat elfogadható, kezelhető, de kiemelt figyelemmel kell kísérni annak változását. Ebben a fázisban a rendszerünk maradhat huzamosabb ideig is, azonban ezek hatásának összeadódása már vezethet katasztrófa állapothoz.

Ezek még nem riasztások, tehát nem számítanak rendkívüli eseménynek, csak a rendszer működése során keletkezett figyelmeztetésnek. [98] [99]

Katasztrófa állapot

A szoftver az előzetesen azonosított súlyos kockázati tényezőt érzékel, amely már önmagában is akár a rendszer leállásával, meghibásodásával, működésében súlyos következménnyel járhat. Extrém esetben a rendszer teljes leállását is ide sorolom.

A program riasztásokat ad, megkísérli legalább a csökkentett üzemben történő maradást, külső riasztásokat ad az együttműködő szervezetek számára. [98] [99]

Visszaállási állapot

A katasztrófa állapotot követően a rendszer már stabil állapotban van (például a szerverek alapbeállításai megtörténtek) és a normál állapotba kell visszaállni. Nem tapasztalható a katasztrófa állapotot előidéző külső tényező. A visszaállítási sorrendnél prioritást kell felállítani, ami egyrészt figyelembe veszi, hogy a kritikus elemek minél hamarabb kerüljenek stabil állapotba, másrészt azonban nem szabad figyelmen kívül hagyni a technológiai, logikai folyamatokat sem. Sajnos a vállalatok túlnyomó része, de még a létfontosságú létesítmények egy része sem rendelkezik incidenskezelési eljárásrenddel (tervvel), ami pedig a szoftvernek is része kell, hogy legyen. [98] [99]

Rendszer kivezetési fázisa

A létfontosságú rendszerelem az üzletfolytonosság vagy a törvényi feltételek folyamatos biztosítása érdekében úgy áll le, adja át a másik kritikus rendszerelemnek (vagy másik vezérlőnek) a működését, hogy ne sérüljön a rendelkezésre állás, sértetlenség és a bizalmasság elve. A program ekkor már bizonyos adatokat nem vesz figyelembe, mert már nem biztos, hogy minden eleme működik a felügyelt rendszernek. Ugyanakkor figyelmeztet, amennyiben a leállítási sorrend katasztrófához vezethet. [98] [99]

4.3. ADATKÖZPONT KIALAKÍTÁSA

Kutatásom kezdetén célként fogalmaztam meg egy felügyeleti és beavatkozó rendszer alapkritériumainak meghatározását, valamint az üzemeltetéshez szükséges jogszabályok körülírását. Mindkettőhöz fontos az adatközpont paramétereinek a pontos ismerete. Az adatközpont kiépítésekor hasznos ajánlás a DCA Certification Guidelines for Data Centres[104] és az adatközpontok harmóniájával foglalkozó LEED[105] minősítés.

Az adatközpontok tanulmányozása során a szakirodalom olvasása mellett, lehetőségem volt megbeszéléseket folytatni Deliága Ákossal, aki több magyarországi, szingapúri és egyéb dél-kelet ázsiai országokban vett részt adatközpontok kiépítésében. Az általa átadott információkat nagymértékben felhasználtam a munkám és kutatásom során. A munkámból adódóan több magyarországi és külföldi adatközpontot is

[104] DCA ((Data Centre Alliance) Certification Guidelines for Data Centres) Adatközpontokkal hitelesítési eljárások
[105] LEED (Leadership in Energy and Environmental Design) – Energia és környezetvédelmi ajánlás

meglátogattam, közöttük a 2017-ben átadásra kerülő NATO HQ[106]-t kiszolgálót is. Továbbá lehetőségem volt egy adatközpont tervezési és kivitelezési munkálataiban is vezető szerepet vállalni.

Minden kritikus információs infrastruktúra rendszer lelke az adatközpont. A továbbiakban ezt az egy elemet vizsgálom, figyelembe véve a kapcsolódását és hogy nem egyedül létezik a rendszerben. Az adatközpont helyes kialakítása alapfeltétel a kritikus informatikai rendszerek biztonságos üzemeltetéséhez, mert az egyik legfontosabb rendszereleme az információs infrastruktúrának. Az információk összegyűjtése mind hozzájárul a kritikus informatikai rendszer biztonságosabb üzemeltetéséhez. A technika-ember-környezet hármasból a technika és a környezet is megjelenik a felsorolásban. Az infrastrukturális elemek (szerverszoba, épületek, helyiségek) a környezetet jelentik, amelyeket összevetve a technikával (hardverek, szoftverek, IT hálózatok) többdimenziós modellt alkalmazva hálózatelméleti elemzéseket végezhetünk el akár a döntéstámogató rendszer segítségével. Ezeket az alapadatokat használja a kockázatelemzés módszertana is, így kiemelt fontosságúak ezek az adatok. [100] [101] [102]

Az adatközpont üzemeltetéséhez rendelkezni kell minden olyan dokumentummal, amely biztosítja a folyamatos és biztonságos üzemeltetést.

Az adatközponton belül különböző helyiségeket különböztetünk meg:

- számítógéptermet, (szerverterem, gépterem);[107]
- szerverszobát;[108]
- rejtjelző helyiségeket;
- távközlési fogadó;
- kommunikációs helyiséget,
- szünetmentes ellátást biztosító helyiséget;
- aggregátor helyiség (legtöbb esetben védett, kültéri elhelyezés);
- klímakiszolgáló helyiség;
- tűzoltó rendszert ellátó és vezérlő helyiség;
- raktárokat;
- műhelyeket;

[106] NATO HQ (NATO Headquarters) NATO központ
[107] Infrastrukturális háttérrel rendelkező helyiség.
[108] Jellemzően kicsi és infrastrukturális háttérrel nem rendelkező helyiség.

- felügyeleti és vezérlő helyiségeket (Operátor helyiség);
- közlekedőket;
- biztonsági felügyeletet ellátó helyiség (közvetetten tartozik ide);
- egyéb kiszolgáló helyiségeket. [96] [103]

Nagyon fontos elemei az adatközpontnak az informatikai rendszereket alkotó eszközök fizikai, valamint technikai jellemzői. Az infrastrukturális hálózatot ezen rendszerelemekkel együtt építik fel, így komplexen kell ezeket kezelni, mert hatással vannak egymásra. Ide tartoznak a:

- kiszolgáló eszközök;
- kliensállomások;
- adattárolók, adattároló médiák;
- mentési rendszerek;
- hálózati aktív és passzív eszközök;
- rack szekrények;
- tápellátás biztosító szünetmentes berendezések;
- aggregátorok;
- légtechnikai berendezések;
- klímaberendezések;
- közműhálózatok;
- berendezések zajszintjei és rezgés jellemzői;
- villámvédelem, vízvédelem;
- felügyeleti, biztonsági és tűzjelző berendezések paraméterei. [96] [102] [103]

Közvetve idetartoznak még:

- eszközök javítására karbantartására szolgáló berendezések;
- szerszámok;
- a dokumentációk (kezelési utasítás, biztonsági utasítás, garancia papírok, licenszek, szerződések, utasítások stb.), amelyek lehetnek papíralapon, vagy elektronikusan tárolva. [96] [104] [105]

A hardverek mellett természetesen foglalkozni kell a szoftverekkel is, amelyek a rendszer és az üzleti folyamatok működtetéséhez szükségesek:

- operációs rendszerek;

- mentőszoftverek;
- kommunikációs szoftverek (levelező, üzenetküldő stb.);
- vírusvédelmi szoftverek;
- határvédelmi rendszerek;
- végpontvédelmi szoftverek;
- felügyeleti szoftverek;
- napló gyűjtő és elemző szoftverek;
- titkosító és rejtjelező szoftverek;
- irodai alkalmazások, vagy programcsomagok;
- üzleti folyamatokat támogató szoftverek: web alkalmazás, adatbázisok; csoportmunkát és folyamatokat támogató szoftverek; adminisztrátori segédprogramok. [96] [103]

Mint az már a rendszer fogalmának meghatározásakor is látható volt tisztázni kell, hogy a rendszerünk milyen környezetben van elhelyezve. Ennek megfelelően érdekesek számunkra az éghajlati viszonyok, talajszerkezet, a területi elhelyezkedés, amely mind-mind befolyásolja a rendszerünk működését, így amennyiben lehetséges sok minden más között objektívan meg kell határozni a gazdasági és politikai viszonyokat, biztonságpolitikai szempontokat. Fontos az objektum távolsága lakott településtől, a népsűrűség, a forgalom, az életszínvonal, a közlekedés. A területre jellemző, környezetre vonatkozó statisztikai adatok lekérése szintén lényeges lehet, ilyenek például a földrengés, az árvíz, a tűzvész, a viharok (tornádó, hurrikán), a hőmérsékleti adatok, a napsütéses órák száma, a hó adatok. A tengerszint feletti, illetve a földszinthez viszonyított elhelyezkedés is meghatározó lehet. A fizikai és környezeti elhelyezkedés szempontjából a védelmi képességek meghatározásához is gyűjteni kell adatokat, hogy később ki lehessen alakítani a fizikai, elektronikai és az élőerős védelmet. Fel kell mérni milyen kommunikációs csatorna érhető el a kapcsolattartáshoz, azok milyen stabilok, megbízhatóak. Fontos, hogy milyen közműhálózattal kell számolni. Van-e lehetőség a valóban független (nyomvonalú) betáplálásokra a víz, a gáz, az erősáram vagy egyéb más energiaellátás tekintetében, továbbá, hogy ezek mennyire megbízhatóak. Meg kell vizsgálni a logisztikai utak állapotát, teherbíró képességüket, az időjárás és egyéb veszélyeknek való kitettségüket. Végül, de nem utolsó sorban fel kell mérni a környezetvédelmi szempontokat is például, hogy milyen előírásokat kell az adott helyszínen figyelembe venni. [26] [96] [103]

Miután rendelkezésre állnak a felmérés adatai, meg kell határozni, milyen jellegű adatközpontot szeretnénk építeni. Az adatközpontokat a rendelkezésre állás szempontjából az Uptime Institute TIER[109] ajánlása szerint négy csoportba sorolhatjuk, ahol mindig a leggyengébb láncszemet kell figyelembe venni:

	TIER I	**TIER II**	**TIER III**	**TIER IV**
Aktív kiszolgáló egységek	N	N+1	N+1	2(N+1)
Ellátási útvonal	csak 1	csak 1	1 aktív, 1 tartalék	2 aktív
Szolgáltatáskiesés nélkül karbantartható	nem	nem	igen	igen
Hibatűrő	nem	nem	nem	igen
Független ellátási útvonalak	nem	nem	nem	igen
Folyamatos hűtés	Terhelésfüggő	Terhelésfüggő	Terhelésfüggő	Biztosított
Rendelkezésre állás	99,671%	99,749%	99,982%	99,995%
Éves leállás és kiesett idő	28,8 óra	22 óra	1,6 óra	0,4 óra

1. táblázat TIER besorolások összefoglalása
(Saját szerkesztés az adatközpont fogalomtár alapján [26] *6.o.)*

- TIER I: Egyirányú energiaellátás, redundancia nélkül;
- TIER II: Egyes elemei tartalékkal rendelkeznek;
- TIER III: Leállás nélkül karbantartható;
- TIER IV: Hibatűrő infrastruktúra. [26] [96]

A kiépítésnél figyelembe kell venni a jogszabálynak megfelelő falak anyagát, vastagságát, a mennyezet és padlózat teherbíró képességét, az épület alapozását, vízáteresztő képességét, az ajtók, ablakok méreteit, biztonsági jellemzőit, EMC[110] jellemzőket az elektromágneses kisugárzás elleni védelem miatt. Dokumentálni kell az alaprajzot, a talaj szerkezetét, az alatta lehetséges vízfolyásokat, az épület tájolását, más épületektől való távolságát, az oda vezető utak állapotát, az épületre ható lehetséges környezeti hatásokat; az épületen belüli funkcionális helyiségeket körülvevő helyiségek megnevezését; az épület állapotát. [96]

[109] Első, másodig, harmadik, negyedik szint. Az Amerikai Telekommunikációs Ipari Szövetség által kiadott adatközpontra vonatkozó szabványban leírt szintek.
[110] EMC (ElectroMagnetic Compatibility) Elektromágneses összeférhetőség

Már a tervezési fázisban fontosak a szakági együttműködések, mert csak úgy garantálható, hogy igazodjanak egymáshoz az épület sajátosságai, a hűtés, a gépészet és az informatikai rendszerek. Mint minden más területen itt is kiemelt szerepet kap, hogy a kivitelezés minden fázisa dokumentált legyen. Ennek megfelelően a beüzemeléskor rendelkezni kell az adatközpont dokumentációi mellett a különböző szakágakra vonatkozó víz, csatorna, fűtés, hűtés, szellőzés, tűzoltó, riasztó rendszerek teljes elrendezési, működési és együttműködési dokumentációival. Az átláthatóság és a dokumentációkkal való megfeleltetés érdekében, valamint az esetleges incidenskezelés miatt fontos a jól látható feliratozás a rendszerelemeken, amelyeket a rendszerünkben is rögzíteni kell. [96]

A helyiségek fűtését vízmentes fűtéssel kell megoldani, például meleg levegő befújással.

A légkondicionálást ipari precíziós berendezésekkel kell kialakítani, amely képes 7x24 órás működésre. A magas követelmények miatt, 2N hűtési rendelkezésre állással kell méretezni a klímaberendezéseket. Egy elem kiesése esetén a rendszer biztosítsa a kritikus terheléskor leadott hő visszahűtését és ezt a klímaberendezést vezérlő automatika külső beavatkozás nélkül legyen képes megtenni. A berendezések működéséhez automatikus szabályozással biztosítani kell a 22±1 °C-ot úgy, hogy a helyiség alkalmas legyen akár tartós munkavégzésre is. Ehhez folyamatosan szűrt friss levegőt, valamint huzatmentes légáramlást is szükséges biztosítani. A legjobb hatásfok érdekében ki kell alakítani egy lezárt hideg folyosót a rack szekrények között. A folyosóhoz menő hideg és meleg elvezető csövek nem akadályozhatják az üzemeltetést és nem keletkezhet rajtuk kondenzvíz. A hideg folyosóban folyamatosan biztosítani kell a megadott 22±1 °C-ot, valamint a 50±10% relatív páratartalmat a legmagasabb terhelések esetén is. A korábban felmért környezeti hatásokból meg lehet határozni 100 éves időtartamra visszamenőleg a külső hőmérsékleti hatásokat és ezzel, valamint a telepítendő eszközökkel, az adott légköbméterrel kell méretezni a hűtési teljesítményt. A klímaberendezés nem várt leállása azonnali riasztást kell, hogy eredményezzen. [96]

A zajterhelés nem haladhatja meg az érvényben lévő szabványok szerinti értékeket. A szerverteremben és környezetében működő gépészeti berendezések (pl. aggregátor, klímahűtő stb.) káros hatásait csillapítani kell elektronikai kisugárzást elnyelő, visszaverő szigeteléssekkel, valamint a rezgések csillapítására helyi rezgéscsillapító megoldásokat kell alkalmazni. [96]

Annak érdekében, hogy a fenti kritériumok teljesüljenek különböző szenzorokat kell elhelyezni a födémben, az aljzatban, a falakon. [96]

A magas rendelkezésre állás miatt, az összes redundáns kiszolgáló rendszerhez hasonlóan az áramellátásnál is biztosítani kell a két független ellátási nyomvonalat. Ez a külső szolgáltatóra és az adatközponthoz vezető tápellátási nyomvonalra is vonatkozik. A két független nyomvonal vezérlésére automatikus kapcsolót kell kiépíteni. A folyamatos működés és a független áramellátás miatt, aggregátor beépítése is szükséges, amely szintén automatikusan indul/leáll és veszi át az áramellátás szerepét váratlan leállás esetén. Az áthidalási időben az energiaellátás biztonsága érdekében magas rendelkezésre állású, a 2N UPS-t kell alkalmazni. Az energiaellátó rendszereknek biztosítani kell az adatközpont folyamatos üzemeltetéséhez szükséges minden berendezés energiaigényét. A kritikus berendezések egyedi villamos tápellátását szervertermen belül is független útvonalakon, önálló kismegszakítókkal ellátva kell biztosítani egészen a berendezésekig, ahol a redundáns tápegységek fogadják azokat. A teljes elektromos hálózatnak meg kell felelni a vonatkozó szabványoknak és jogszabályoknak. [96] [106]

Az épületbe történő be- és kilépést automatikusan működő rendszerrel kell ellátni. Az áthaladást mindkét irányban és minden esetben regisztrálni kell, ennek elkerülését fizikailag meg kell gátolni. Ennek érdekében egy személy áthaladását kikényszerítő sorompót, forgóvillát kell alkalmazni, amelyet reagáló erőkhöz kell bekötni. Amennyiben az adatközpontban személy nem tartózkodik, a riasztórendszert automatikusan élesíteni kell. Zárt láncú kamerarendszerrel kell ellenőrizni a belépő pontokon a mozgásokat. Az elektronikai rendszer kiváltható állandó élő erős védelemmel, akik a regisztrálást is elvégzik. A reagáló erők munkáját segíti elő a zárt láncú kamerarendszer, amelyek segítségével a riasztások ellenőrzése mellett a biztonsági zóna, kerítések, folyosók kiszolgáló helyiségek, vagy az épületen kívüli területek megfigyelése történik. A kamerarendszert ki kell egészíteni biztonsági világítással, amely alkalmas lehet a menekülő útvonalak megvilágítására is. [96]

Szintén fontos elektronikai védelmet biztosít az elektronikai jelzőrendszer, amely felügyeli a biztonsági területet, a kiszolgáló helyiségeket, valamint az ott található összes nyílászáró szerkezetet, falazatot, mennyezetet, padlózatot. A védelemnek ki kell terjedni a kiszolgáló infrastruktúra elemeire is. A riasztás a

helyszínen történő jelzés mellett közvetlenül értesíti a reagáló erőt is. A jelzőrendszerek a behatolások mellett a füst, tűz, vízbetörés, páratartalom változást is jelzik. [96] [107]

A szervertermet és a kiszolgáló helyiséget különálló tűzvédelmi zónaként kell kezelni, így ezek független tűzjelző és automatikus működtetésű oltórendszer kiépítéssel kell, hogy rendelkezzenek. Az tűzjelző rendszer VESDA[111], vagy azzal egyenértékű aspirációs rendszerrel kell megvalósítani. Tűz esetén a riasztórendszer a helyszínen történő riasztás mellett közvetlenül értesítse a reagáló erőt is, és biztosítani kell a szellőzés és a klímaberendezés tűzcsappantyúinak szelektív zárását. Az automatikus tűzoltás beindulását lehetőség legyen emberi beavatkozással megakadályozni. Az oltórendszert úgy kell kialakítani, hogy az oltás hatására az informatikai rendszerek ne sérüljenek. Az oltás beindítása előtt a szerverek kezdjenek automatikus mentésbe, majd álljanak le. Az elektromos ellátórendszer kábelei tűzálló minősítéssel rendelkezzenek. [26] [96]

A beépített hardver és szoftverelemek tekintetében is teljes körű kompatibilitás szükséges. A kiépítéskor a beszállítóktól megfelelőségi nyilatkozatot kell kérni, amellyel igazolják, hogy a berendezések megfelelnek a gyártói előírásoknak és a vonatkozó szabványoknak. A kompatibilitásnak ki kell terjedni az informatikai rendszerekre, a kiszolgáló rendszerekre, az infrastruktúrára és az együttműködő rendszerekre is. A kiválasztásnál nagy gondot kell fordítani a későbbi beszerezhetőségre, a magasabb szintű támogatásra, a biztonságra és a személyzet szaktudásának meglétére, esetleges képzési lehetőségére. A beszállítónak biztosítani kell, hogy az eszközök rendelkezzenek olyan interfészekkel, amelyek biztosítani tudják a felügyeleti rendszerek számára a folyamatos információkat. [96]

Az adatközpont(ok) a georedundancia követelménye miatt fizikailag kettő vagy több helyszínen épül(nek) ki, de virtuálisan egy egészként is kezelhetők. Egy adatközpont, szerverterem kiesése esetén az üzletmenet folytonosság és a magas rendelkezésre állás miatt, biztosítani kell egy tartalék rendszer meglétét is. A meghatározott rendelkezésre állást követően lehetőség van eldönteni, hogy milyen típusú tartalékképzést választunk, amihez igazítani kell a felügyeleti és beavatkozó rendszert is. [96]

[111] VESDA (Very Early Smoke Detection Apparatus) – Korai füstérzékelő berendezés

Amennyiben a hideg tartalékképzést választjuk, akkor az alacsony költség mellett szerződésekkel tudjuk biztosítani, hogy amennyiben valamilyen eszköz, illetve a teljes rendszer meghibásodik, viszonylag rövid időn belül szállítsák és üzemeljék be az új kiszolgáló rendszert, vagy a rendszernek egy elemét. Ennek egyik változata, amikor a szerződés szerint a szállítandó eszközök lekötése mellett, rendelkezésre áll egy megfelelő kapacitású működési környezet, amely átveszi a kiesett szerepét. [96]

A másik lehetőség, amikor már rendelkezésre áll az összes hardverelem a raktárban, melynek előnye, hogy viszonylag hamar pótolható a kiesett elem. Hátránya, hogy legtöbb esetben feleslegesen állnak az eszközök használaton kívül a raktárban, így költséghatékonyság miatt nem a legjobb megoldás. [96]

A harmadik lehetőséget meleg[112] megoldásnak nevezem, amikor már órákon belül visszaállítható a normál működés. Ez két úton érhető el, egy mobil egység, vagy egy „hot site" áll rendelkezésre. Ebben az esetben a rendszer ki van építve, már csak az éles adatokat kell visszahozni a mentésből, vagy átmásolni egy tartalék site-ról. [96]

Végül, amikor az éles és a tartalék rendszer is folyamatosan üzemel párhuzamosan, az adatok mindkét rendszeren megtalálhatóak. Kritikus infrastruktúráknál minden esetben ez a megoldás alkalmazandó. Ennek a gazdaságosabb változata, amikor mindkét oldal éles üzemben megy terheléseloszlással, és az egyik kiesése esetén a másik „automatikusan" képes átvenni a leállt szerepét. Ennek egy változata, amikor az egyik site[113] egy mobil[114] adatközpont. Sok esetben ez lehet a tökéletes megoldás, mivel a mobilitással minősített időszakban [115] (illetve azt megelőzően) egy működő rendszert telepíthetünk védett helyre. Ebben az esetben az üzemeltetők tökéletesen ismerik a rendszert, amelynek nincs felfutási ideje, vagy a beüzemelés alatti váratlan esemény.

A NATO AJP-6 dokumentum még a rendszer robosztusságát említi, mint lehetőség, amennyiben növelni akarjuk a rendelkezésreállást, ellenállóképességet a nem kívánt hatásokkal szemben. [83]

A telekommunikációs és hálózati összeköttetések esetén szintén redundanciát kell alkalmazni.

---

[112] A meleg és hideg megoldás az eszközök üzemeltetése során keletkezett hőmérsékleti jellemzőére vezethető vissza. Amennyiben egy eszköz nem működik, nem termel hőt, így ez lesz a hideg.
[113] Site jelentése ebben a környezetben: fizikailag (helyileg) elkülönült rendszerelem, adatközpont.
[114] Viszonylag rövid idő alatt áthelyezhető egy másik helyszínre, ahol szintén rövididő alatt üzembehelyezhető.
[115] Minősített időszakok (Magyarország Alaptörvénye szerint): rendkívüli állapotot, szükségállapot; megelőző védelmi helyzet, terrorveszélyhelyzet, váratlan támadás, vészhelyzet.

Ahhoz, hogy a visszaállítás megtörténhessen mentési és visszaállítási stratégiát kell készíteni a hardverekre éppúgy, mint a szoftverekre, az adatokra és a hálózati elemekre egyaránt. Ehhez a biztosítani kell a megfelelő személyzetet, a felkészülést, a szabályzókat és a tesztelési lehetőséget.

A visszaállási terv hatással lehet az üzletmenet folytonosságra (BCM[116]) is a szolgáltatás folytonosságon keresztül. Kiemelkedően kritikus szolgáltatások esetében lehetőség van külső szolgáltatókkal szerződést kötni, akik a visszaállás idejére biztosítják a szolgáltatást.

Egyes magyarországi kritikus információs infrastruktúrának a másodlagos adatközpontját el lehet helyezni központi adatközpontokban, ahol privát felhő szolgáltatásként lehet biztosítani az üzletmenet folytonosságot, a magasabb rendelkezésreállást.

4.4. KOCKÁZATELEMZÉS

„Minél többet tudunk arról, mennyi minden romolhat el sejtjeinkben, annál nagyobb csodának tűnik, hogy időnként mégis egészségesek vagyunk."

Forrás: [108] 261. o.

A kockázatelemzésnek több célja is lehet. Az egyik a biztonság növelésé, amikor megvizsgáljuk, hogy milyen fenyegetésekkel, sérülékenységekkel számolhatunk és ezeket a kockázatokat elemezve eldönthetjük, hogyan reagálunk azok esetleges bekövetkezésekor. A másik lehetőség, hogy az üzemeltetéshez, például a karbantartáshoz, vagy a rendszer állapotváltozásokhoz végezzük el a kockázatelemzést. Azonban a kettő között vannak átfedések, összefüggések is.

„Kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése."

Forrás: [18] 1. §

Az elektronikus információkkal és a létfontosságú rendszerek védelmével kapcsolatban több jogszabály is említést tesz a kockázatalapú védelemről, amelynek fontos része a kockázatelemzés is. A kockázatelemzésnél figyelembe kell venni a vagyonelemeket, fenyegetettségeket, sérülékenységeket és felmerülő zavaró

[116] BCM (Business Continuity Plan) Üzletmenet-folytonossági terv

eseményeket. Ekkor ki lehet alakítani egy képet a rendszerről normál működés esetére és a várható események hatására kialakult helyzetekre. Ezeket az adatokat felhasználva dinamikus kockázatelemzést kell végrehajtani, ami szintén a rendszer része kell, hogy legyen. A rendszerünk üzemeltetéséhez el kell készíteni a kockázatkezelési tervet.

A kockázatelemzés egy igen komplex feladat, a mélységét tekintve pedig szinte meghatározhatatlan. Mint a hálózatelméletnél és a modellalkotásnál is megfogalmaztam, igen nehéz meghatározni azt a mélységet, amit még érdemes és szükségszerű bevonni az elemzésbe. A kutatás és a munkám során az ISO/IEC 27000 szabványcsaládot használtam, amely egy jól kezelhető dokumentumegyüttesnek bizonyult. Ezen belül az ISO/IEC 27005 foglalkozik konkrétan az információbiztonsági kockázatkezelési eljárásokkal. Azonban figyelembe vettem az ISO/IEC 20000 szabványban leírtakat is. Fontos, hogy az ajánlások alapvetően jó kiindulási alapok, de az adott szervezetre alkalmazandó módszert ki kell dolgozni.

4.4.1. ALAPADATOK

A kockázatok értékeléséhez alapinformációkra van szükség, mint minden döntés meghozatalánál, ez követelmény. Ahhoz, hogy minden lehetséges információval rendelkezzünk, össze kell gyűjteni a jogi szabályzókat, a szervezet saját szabályzatait, az ajánlásokat és a szabványokat is. Rendszerintegrátoroktól, gyártóktól be kell szerezni az információkat a termékekkel kapcsolatban. Az itt összegyűjtött adatok több szempontból is fontosak az üzemeltetés szempontjából. A kockázatelemzés mellett ezek szükségesek a CMS rendszernek is, amelyeket a kutatásom során szintén tanulmányoztam.[117]

4.4.1.1. HATÓKÖR

Meg kell határozni a vizsgált rendszer értelmezési tartományát. A rendszer működtetéséhez szükség van tőle „független” rendszerekre is, mint például az energiaellátó rendszer. A kockázat felmérésekor számolunk ugyan velük, de csak, mint a külső tényezővel. Azok rendszerelemeit nem tudjuk figyelembe venni, csak, mint külső rendszer egészét, mivel nincs ráhatásunk a működtetésükre. Így határvonalat képezünk, meghatározzuk az átadási pontokat és feltételeket. [109]

[117] Ennek részletezése megtalálható a 3.7. részben.

4.4.1.2. SZERVEZETI ÉS ÜZLETI FOLYAMATOK

Minden esetben egy szervezet működésekor létezik az üzlet sikeressége, vagy a közszférában a feladat végrehajtása érdekében működő (üzleti)folyamatok és adatok. Természetesen ezek folyamatosan változnak a környezeti hatásokra adott válaszok szerint, de fontos, hogy ezeket pontosan definiálni lehessen a felmérés időszakában. A felmérés során modellezni kell a szervezet működéséhez szükséges üzleti folyamatokat. Itt lehetőség nyílik az egyes területeken egyszerűsítésekre, racionalizálásokra is. Erre azért is szükség lehet, mert ezek a folyamatok már magában is kockázati elemként léphetnek fel és folyamatos visszacsatolások révén ebben a fázisban is javítható a rendszer működése (PDCA). Az ISO/IEC 27005-ben a folyamatok és az adatvagyonok, mint elsődleges vagyonelemek jelennek meg. [109] [110]

4.4.1.3. VAGYONFELMÉRÉS

A vagyonfelmérésnél össze kell gyűjteni a fentebb már említett információkat úgy, mint a jogi hátteret, működési környezetet, pénzügyi erőforrás rendelkezésre állására vonatkozó adatokat, üzleti folyamatokat.

Az adatokat tekintve fel kell mérni az úgynevezett adatvagyont, amennyiben veszteségalapú kockázatelemzést szeretnénk vizsgálni „be kell árazni” az egyes adatot, információt. A könnyebb kezelhetőség érdekében osztályozni kell őket, így több csoportba sorolhatók a beárazott adatok, információk, amelyek az üzleti folyamatok be- és kimeneti értékei lesznek. [76] Hasonlóan képviselhetnek értéket a számítógépes alkalmazások, ahol az adat és a folyamat alkotja az értéket. Ide kell érteni a szervezet által kezelt dokumentumokat is, amelyeket osztályozni kell. Egyfajta osztályozás a minősítési szint is, amelyet ebben az esetben fel kell használni. [19] [109]

ÉPÜLETEK

Alapvető vagyonelem az infrastruktúra elemei. Ide tartoznak a kiszolgáló épületek, amelyek már a korábban leírt jogszabályok[118] szerint is kategorizálhatók.

Az épületeken belül megkülönböztetünk a már korábban felsorolt [119] adatközpontot, számítógéptermet, (szerverterem, gépterem), rejtjelező helyiségeket

[118] 90/2010. (III. 26.) Korm. rendelet; 41/2015 BM rendelet.
[119] lsd: helyiségek (3.3 Adatközpont kialakítása)

stb.[120] Ezek az objektumok rendelkeznek az ott felsorolt paraméterekkel, amelyek fontosak lehetnek a kockázatelemzésnél. A felsorolt adatokat mind szerepeltetni kell majd a létrehozandó felügyeleti és beavatkozó rendszerben. [109]

HARDVEREK

A következő fontos elem az informatikai rendszerekben az őt alkotó eszközök és fizikai, valamint technikai jellemzői. Ide tartoznak a korábban felsorolt kiszolgáló eszközök, kliensállomások, adattárolók stb.[121] [109]

SZOFTVEREK

A hardverek mellett természetesen fel kell mérni a szoftvereket is, amelyek a rendszer és az üzleti folyamatok működtetéséhez szükségesek.

Ezek a korábban felsorolt operációs rendszerek, a mentőszoftverek, kommunikációs szoftverek (levelező, üzenetküldő stb.), végpontvédelmi szoftverek stb.[122] Itt is nagyon fontos a jellemzők meghatározása, a verziószám, a frissítések dokumentálása. Az egyénileg fejlesztett szoftverek tekintetében gondoskodni kell a pontos dokumentálásról a fejlesztés megkezdésétől a selejtezésig. [109]

HÁLÓZAT

A hardverelemeket összekötő hálózatnál kockázatelemzés szempontból is nagyon fontos a jó dokumentáltság a fizikai és technikai paraméterek meghatározása. Amennyiben a kiépítésnél nem tettük meg, fel kell mérni a hálózati kábelek nyomvonalát, típusát és csatlakozó felületeit. A kommunikációs rack szekrény elhelyezkedése, fizikai technikai paraméterei és a benne elhelyezett aktív és passzív eszközök paramétereit a tervezésnél figyelembe kell venni. Természetesen ide tartoznak a nem vezetékes átviteli utak és azokat létesítő eszközök is, valamint az infokommunikációs eszközök mellett a telekommunikációs eszközök is. [109]

---

[120] lsd: helyiségek (3.3 Adatközpont kialakítása)
[121] lsd.: rendszerelemek (3.3 Adatközpont kialakítása)
[122] lsd: szoftverek (3.3 Adatközpont kialakítása)

KÖRNYEZET

Nem mindegy, hogy milyen környezetben helyezkednek el a fenti rendszerelemek. Számolnunk kell a szintén már korábban felsorolt éghajlati viszonyokkal, talajszerkezettel, területi elhelyezkedéssel stb., de ide sorolom a jogszabályi környezetet is.[123]

SZEMÉLYI ÖSSZETÉTELRE VONATKOZÓ ADATOK

A rendszert üzemeltető és felhasználó személyzet összetétele is meghatározó egy kockázatelemzés szempontjából. Fel kell mérni, hogy a rendszer egészére vonatkozóan mennyi és milyen képzettségű, képességű humán erőforrással számolhatunk, kezdve a vezetőktől a rendszergazdákon át a felhasználókig. A paramétereket tekintve fontos a képzettség, a képesség, a tapasztalat, a megbízhatóság, az életvezetés, a kommunikációskészség, a lojalitás, a kapcsolatrendszer stb. A későbbiekben ezek az entitások[124] is kapcsolhatók más hálózati dimenzióban lévő entitásokhoz.[125] [109]

SZERVEZETRE VONATKOZÓ INFORMÁCIÓK

A fenti személyek valamilyen rendszer szerint vannak összerendelve. Az üzleti folyamatokat, az adatokat, az üzleti célt, az elhelyezkedést, a hardvert/szoftvert és minden előző pontot figyelembe véve kialakul egy szervezeti struktúra a helyes működés érdekében. Ezekhez a pozíciókhoz (és nem a személyekhez) felelősségek és jogok lesznek delegálva. Minden szervezeti elemnek megvan a saját felelősségi köre, amit munkaköri utasításban rögzítenek. A pozícióknak és a szervezeti elemeknek is megvan az együttműködési területe és feltétele, valamint a határvonalak, amelyek behatárolják a mozgásterületet (ezek az átadási pontok is egyben). Vannak kommunikációs útvonalak, amelyeken keresztül az információ áramlik. Ez lehet utasítás, parancs, tájékoztatás, visszajelzés stb. [109] [111] [112]

---

[123] lsd.: környezet (3.3 Adatközpont kialakítása)
[124] Entitás: valamilyen személy, dolog, ami magában foglalja az egyedi tulajdonságainak összességét.
[125] A többdimenziós hálózat jelentőségét az alábbi helyen részleteztem: 2.fejezet. Az ember okozta környezeti hatások.

4.4.1.4. KÖVETKEZMÉNYEK, HATÁSOK

Ahhoz, hogy a kockázatokkal érdemben tudjunk foglalkozni, ismerni kell azt is, hogy mi történik, ha egy nem várt esemény bekövetkezik, a rendszer állapota hogyan változik meg. Ezek a következők lehetnek:

- emberi élet közvetlen veszélyeztetése, vagy egészségkárosítása;
- pénzügyi veszteség;
- hitelesség, megbízhatóság elvesztése pl. szövetségi viszonyokban történő bizalomvesztés, törvényi kötelezettségből adódó megnemfelelés;
- a nukleáris és vegyi létesítmények biztonsági rendszereinek a veszélyeztetése;
- a rendszer állapotának változása;
- stb.

4.4.1.5. PÉNZGAZDÁLKODÁS

Ismerni kell a képességek mellett a lehetőségeket, ezen belül a pénzügyi határokat is. Az előbb felsorolt jellemzőkhöz hozzá kell rendelni a pénzügyi értéküket, számolni kell az értéknövekedéssel, vagy csökkenéssel is. A kockázatelemzésnél érdekes lehet, hogy milyen pénzügyi összefüggések, interdependenciák vannak az egyes elemek között, a dominóhatás hogyan érvényesülhet.

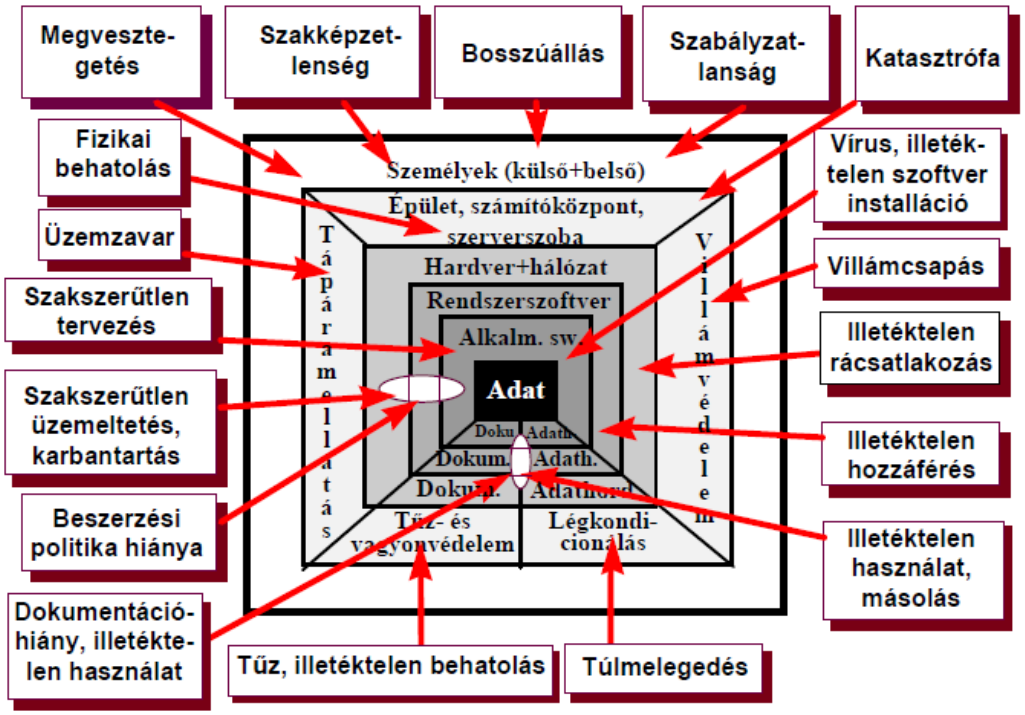
4.4.1.6. CÉLOK

A vagyonfelmérésből, a jogszabályokból, a szervezeti és üzleti folyamatokból meghatározzuk, hogy mi a célunk az informatikai üzemeltetés, biztonság területén, tehát mi az, amit mindenképpen „életben kell tartani”, mi az, amit erősebben kell védenünk, mi az, ami komoly veszteséget okozhat számunkra.

Ezek képezik az alapadatokat, amelyeket össze kell gyűjteni, rendszerezni, dokumentálni, adatbázisba gyűjteni és folyamatosan naprakészen tartani.

4.4.1.7. FENYEGETETTSÉGEK MEGHATÁROZÁSA

A veszélyforrásokat és azok szövevényes hatásait mutatja be az ITB 12. számú ajánlásában található a következő ábra:



9. ábra ITB 12. sz. ajánlása [15] 16. o.

A 7. számú mellékletben megtalálható táblázat pedig csoportosítva sorolja fel a fenyegetéseket, veszényforrásokat. Természetesen a veszélyforrások is minden kritikus informatikai rendszernél változnak. [113]

4.4.1.8. SÉRÜLÉKENYSÉGEK MEGHATÁROZÁSA

A sérülékenységek meghatározásánál a vagyonfelmérés során feltárt elemeket kell megvizsgálni, abból a szempontból, hogy milyen sérülékenységekkel számolhatunk az üzemeltetés során. Ezek általában a helytelenül beállított hardverelemekből, vagy a hibásan konfigurált szoftverekből adódhatnak, de ide tartozhat a hálózatnál a nem megfelelően választott sávszélesség, vagy a protokollok megválasztása is. A szabályok be nem tartása, vagy éppen a nem jól megírt szabályzók is okozhatnak sérülékenységet. A személyekkel kapcsolatban a legnagyobb sérülékenységet a képzetlenség vagy a túlzott elvárások okozhatják. Hasonló problémák lehetnek a szervezet tekintetében a rosszul megválasztott humánerőforrás elosztás, vagy a kommunikációáramlás rossz alkalmazása. Míg a veszélyforrásokat legtöbbször valami külső esemény személy okozza, a sérülékenység pedig a saját szervezet, szoftver, hardver, illetve munkatársak hibájára vezethető vissza. [76]

Fontos azonban ismét hangsúlyoznom, hogy az ajánlásokban, szabványokban felsorolt sérülékenységek csak segítséget nyújtanak és egy általános rendszer esetén használatosak. A sérülékenység tekintetében saját magunknak kell meghatározni mi számít annak, ráadásul pl. az ISO/IEC 27005 szabvány a biztonsági oldalról közelíti meg a kérdéskört, de számunkra az üzemeltetés területén létezhetnek olyan sérülékenységek, fenyegetettségek, amelyek a biztonságot közvetlenül nem befolyásolják. [109]

4.4.2. KOCKÁZAT ÉRTÉKELÉSE

4.4.2.1. MOTIVÁCIÓ

Amennyiben az előbbi szempontok szerint felmértük az egész rendszerünket, már tudunk is válaszolni arra, hogy miért és mennyire lehet érdekes mások számára a szervezetünk/cégünk. Mi az, amit meg szeretnének szerezni, vagy mi az, amivel kárt okoznának nekünk, illetve az üzletmenet folytonosság miatt, miért kell annak a szolgáltatásnak mindenképpen működnie. Továbbá választ kaphatunk arra is, hogy mi motiválhatja az elkövetőket az illegális tevékenység során, amit velünk szemben végeznek. A kockázatkezelés alkalmazásával itt is tehetünk ellenintézkedéseket, illetve felkészülhetünk lépésekre. Különböző motivációk létezhetnek, amelyek hajthatnak embereket, csoportokat. A hackerek például a hírnév, a kihívás, a pénz, az egy csoportba való bekerülés érdekében cselekedhetnek, míg a terroristák, ipari kémek még politikai és vallási megfontolásból tevékenykednek, de a terroristáknak fontos a média hírverés is. [109]

4.4.2.2. KOCKÁZAT ÉRTÉKÉNEK MEGHATÁROZÁSA

A következő példában a valószínűségszintet 5 részre bontottam. A 0 érték az, mikor nagyon valószínűtlen az esemény bekövetkezése, szinte lehetetlen. Ilyen lehet például, hogy Debrecenben vulkánkitörés okozta kár keletkezik. A 4-es érték pedig igen gyakran előforduló eseményt jelenthet, például vírusos adathordozó használata az oktatási intézményeknél. Hasonlóan osztályozom az esemény bekövetkezésének a hatását is, illetve súlyozom 0 és 4 között. 0, amikor semmilyen hatása nincs a rendszeremre, 4, pedig akkor, amikor komoly következménye lesz, pl. a teljes rendszer napokra leáll. Az oszlop és sor keresztezéseibe az így összeadott értékeket írom. Az így

kapott táblázatot (metaadatokat) már fel lehet használni a későbbiekben különböző értékek megadásához. [109]

		Valószínüség				
		nagyon valószínűtlen	valószínűtlen	lehetséges/talán	valószínű	nagyon valószínű
Hatása	nagyon alacsony	0	1	2	3	4
	alacsony	1	2	3	4	5
	közepes	2	3	4	5	6
	magas	3	4	5	6	7
	nagyon magas	4	5	6	7	8
			Magas kockázat			
			Közepes kockázat			
			Alacsony köckázat			

2. táblázat Valószínüségek
(saját szerkesztés)

A COBIT és a 41/2015 BM rendelet szerint a rendszerre gyakorolt hatás (vagy károkozási képesség) szintjeihez hozzárendelik a bizalmasságot, a sértetlenséget és a rendelkezésre állást. Így definiálva lesz, hogy mit jelentenek a szintek ezek tekintetében, illetve így külön-külön is használható a táblázat. [109]

4.4.2.3. KOCKÁZAT AZONOSÍTÁS, ELEMZÉS

FÜGGŐSÉGEK MEGHATÁROZÁSA

A feltárt folyamatokat és a vagyonleltárból nyert adatokat egy mátrixba töltve a keresztezésekbe függőségi indexeket tudunk meghatározni. Tehát megmutatja, hogy egy elem gyengülése, kiesése milyen hatással van az adott folyamatra, ezáltal az üzleti célok megvalósítására. A 3. táblázatban szereplő index értékeinek az intervallumával súlyozhatók a pontozások is, így a későbbi táblázatok összevetésénél priorizálhatók a fontosságok is. Jelenleg százalékos értéknek megfelelő pontot írtam be indexként. Az utolsó oszlopban, illetve sorban összesítettem a pontokat is. A sárga jelölés a legmagasabb (legkritikusabb) értéket mutatja. Így a „Gépház” meghibásodása, kiesése komoly gondot okozhat a szervezet egészére, vagy remélhetőleg a „Munkafolyamat_3_1” nem egy komoly munkafolyamat a szervezet életében, mert több elem is veszélyezteti a sikeres működését. A színek itt is a kockázatok mértékét jelentik, mint az összes táblázatban. [109] [114]

			Vagyonelem										
			Épületek			Hardverek			Szoftverek			...	
			Szerverterem_1	Gépház_1	Munkaterem1	Szerver_1	Router_1	NAS_1	Op.rendszer1	Mentőszoftver	Végpontvédelem	...	Kritikussági érték
Munkafolyamatok	Munkafolyamat1		100	100	0	40	20	10	10	0	0	40	320
	Munkafolyamat2												0
		Munkafolyamat_2.1	0	80	20	20	30	20	20	0	0	20	210
		Munkafolyamat_2.2	40	20	10	60	30	10	40	20	10	40	280
		Munkafolyamat_2.3	20	30	20	80	0	0	20	30	20	0	220
	Munkafolyamat3												0
		Munkafolyamat_3.1	40	100	10	40	60	20	20	100	10	10	410
		Munkafolyamat_3.2	40	20	10	30	100	90	0	0	0	30	320
	...		20	10	20	40	20	10	20	30	20	90	280
Kritikussági érték			260	360	90	310	260	160	130	180	60	230	

3. táblázat Folyamat/Vagyonelem függőség szemléltetés[126]
(saját szerkesztés)

A következő táblázat segítségével azt vizsgálom meg, hogy a veszélyforrások milyen hatással vannak a vagyonelemekre. A 4. táblázat Veszélyek/Vagyonelem függőség szemléltetés) a 2. táblázatnál alkalmazott értékeket írtam be. Így például a „Tűz" hatása a „Szerverterem_1" elemre 8 értéket kapott, mert az elképzelt szervezetnél nagy valószínűséggel következhet be a tűzeset, valamint, ha bekövetkezik szinte biztos, hogy megsemmisül a „Szerverterem_1" elem. Az utolsó oszlopban látható az is, hogy a „Tűz" kapta a legmagasabb pontot a Veszélyforrások közül, így majd a kockázatkezelésnél valószínű, hogy foglalkozni kell vele. Az utolsó sor pedig a „Gépház" veszélyeztetettségét mutatja. [76] [109] [114]

		Vagyonelem										Kritikussági érték
		Épületek			Hardverek			Szoftverek			...	
		Szerverterem_1	Gépház_1	Munkaterem1	Szerver_1	Router_1	NAS_1	Op.rendszer1	Mentőszoftver	Végpontvédelem	...	
Veszélyforrások	Tűz	8	3	1	6	1	6	3	8	0	3	39
	Vízkár	4	7	4	4	1	2	0	2	0	0	24
	Szennyeződés	0	3	0	1	1	2	0	1	0	3	11
	Nagy kiterjedésű, vagy súlyosabb baleset	1	3	0	1	1	2	3	4	0	2	17
	Eszköz, vagy adathordozó megsemmisülése	3	0	0	3	1	8	1	7	2	0	25
	Por, korrózió, fagyás	1	4	0	2	1	2	0	2	0	2	14
	Vulkánkitörés	0	1	0	1	1	2	0	0	0	1	6
	Rendkívüli időjárás	2	7	0	2	1	2	0	6	0	2	22
	Árvíz	5	7	0	6	1	5	0	4	2	4	34
Kritikussági érték		24	35	5	26	9	31	7	34	4	17	

4. táblázat Veszélyek/Vagyonelem függőség szemléltetés[127]
(saját szerkesztés)

Azt, hogy mennyire kell foglalkozni a kockázatokkal, további elemzéseket igényel. Megvizsgáltam, hogy a tűz bekövetkezésekor milyen munkafolyamatok kerülnek veszélybe. Természetesen ez egy nagyon leegyszerűsített következtetés, mert több paramétert és pontosabb számítást igényelne. Hiányoznak korrekciós tényezők és rendszerelemek egymásra gyakorolt hatását sem vettem figyelembe. Az utóbbi a dominóeffektus miatt teljesen váratlan eseményeket idézhet elő. Ehhez modellezni kell, és algoritmusokat írni a számításhoz. Az értékeket a 3. táblázat Folyamat/Vagyonelem függőség szemléltetés és a 4. táblázat Veszélyek/Vagyonelem függőség szemléltetés

[126] A jobb olvashatóság érdekében a táblázat megtalálható a 8. számú mellékletben is.
[127] A jobb olvashatóság érdekében a táblázat megtalálható a 8. számú mellékletben is.

megfelelő celláinak átlaga adta. Az eredményből látszik, hogy egy tűz, vagy egy baleset bekövetkezésekor rendszer elemektől „függetlenül” a „Munkafolyamat_3_1” sérülhet meg leghamarabb. (lásd: 5. táblázat) [76] [109] [114]

Tűz		
Munkafolyamat		Kockázat
Munkafolyamat1		157
Munkafolyamat2		0
	Munkafolyamat_2.1	65
	Munkafolyamat_2.2	124
	Munkafolyamat_2.3	105
Munkafolyamat3		0
	Munkafolyamat_3.1	194
	Munkafolyamat_3.2	130
…		110

Nagy kiterjedésű, vagy súlyosabb baleset		
Munkafolyamat		Kockázat
Munkafolyamat1		59
Munkafolyamat2		0
	Munkafolyamat_2.1	43
	Munkafolyamat_2.2	49
	Munkafolyamat_2.3	37
Munkafolyamat3		0
	Munkafolyamat_3.1	96
	Munkafolyamat_3.2	47
…		49

5. táblázat Kockázat értékelése
(saját szerkesztés)

Egy nagyon fontos módszer még a vagyonelem súlyozása. Ekkor a 4. táblázat Veszélyek/Vagyonelem függőség szemléltetés- kiegészítettem a Vagyonelemeket a szervezet számára képviselt értékével. Ezt a számot szorzom meg a Veszélyforrás és Vagyonelem metszetében lévő értékkel. A 6. táblázatban látható, hogy helyenként érdekesen átrendeződik színezés. Ebből is látszik, hogy mennyire fontos szempont és mennyire ki kell értékelni a vagyonelemek értékével együtt a rendszerünket. Nem mindegy, hogy mekkora kárt okoz a veszélyforrás, milyen erőforrás ráfordításokkal (pl.: humán, anyagi stb.) lehet azt helyreállítani. [76] [109] [114]

		Vagyonelem																				
		Épületek					Hardverek						Szoftverek						…			
1-800		Szerverterem_1		Gépház_1		Munkaterem1		Szerver_1		Router_1		NAS_1		Op.rendszer1		Mentőszoftver		Végpontvédelem		…		Kritikussági érték
801-1600		Értéke (1-300)																				
1601-2400		299		101		40		180		90		240		120		300		280		10		
Veszélyforrások	Tűz	8	2392	3	303	1	40	6	1080	1	90	6	1440	3	360	8	2400	0	0	3	30	8144
	Vízkár	4	1196	7	707	4	160	4	720	1	90	2	480	0	0	2	600	0	0	0	0	3977
	Szennyeződés	0	0	3	303	0	0	1	180	1	90	2	480	0	0	1	300	0	0	3	30	1364
	Nagy kiterjedésű, vagy súlyosabb baleset	1	299	3	303	0	0	1	180	1	90	2	480	3	360	4	1200	0	0	2	20	2929
	Eszköz, vagy adathordozó megsemmisülése	3	897	0	0	0	0	3	540	1	90	8	1920	1	120	7	2100	2	560	0	0	6252
	Por, korrózió, fagyás	1	299	4	404	0	0	2	360	1	90	2	480	0	0	2	600	0	0	2	20	2247
	Vulkánkitörés	0	0	1	101	0	0	1	180	1	90	2	480	0	0	0	0	0	0	1	10	857
	Rendkívüli időjárás	2	598	7	707	0	0	2	360	1	90	2	480	0	0	6	1800	0	0	2	20	4057
	Árvíz	5	1495	7	707	0	0	6	1080	1	90	5	1200	0	0	4	1200	2	560	4	40	6366
Kritikussági érték		24	7176	35	3535	5	200	26	4680	9	810	31	7440	7	840	34	10200	4	1120	17	170	

6. táblázat Káralapú számítás[128]
(saját szerkesztés)

A kutatásom során különböző szoftvereket vizsgáltam, amelyek segítségével elvégezhetők a kockázatelemzések. Ilyen szoftver volt például a PILAR[129], amelyet a

[128] A jobb olvashatóság érdekében a táblázat megtalálható a 8. számú mellékletben is.
[129] http://www.pilar-tools.com/en/index.html; A PILAR-Tools képernyőképe megtalálható a 6. számú mellékletben.

Spanyol Nemzeti Biztonsági Felügyelet támogat, illetve megtalálható az ENISA oldalán is, mint támogatott alkalmazás. [115] [116]

4.4.1. KOCKÁZATKEZELÉS

Az adatokból és információkból, melyeket az elemzés során feltártunk, rendszereztünk és feldolgoztunk egy jelentést kell készíteni, melyet a döntéshozóknak be kell bemutatni. A dokumentumnak a célközönség számára is érthetőnek kell lennie, a kockázatok ismertetése mellett legyenek benne javaslatok, elvi ellenintézkedési tervek, érvelések. A vezető –lehet, hogy a többi, számunkra ismeretlen információval történő együttes mérlegelést követően – meghozza a döntését, hogy mi történjen a feltárt kockázatokkal, amelyet ezután betáplálhat a felügyelő és beavatkozó rendszerbe. [76]. A következő döntések születhetnek meg:

- Csökkentés

  A legkézenfekvőbb döntés, hogy ha már ismerjük a problémát, annak hatását, akkor szüntessük meg vagy csökkentsük a kockázatot. A csökkentésre lehet példa, hogy a tűzjelző és tűzoltó rendszert korszerűsítsük, vagy a védendő terület környezetét tisztítsuk meg az éghető anyagoktól.
- Elkerülés

  A kockázatokat el is kerülhetjük. Erre példa, amikor a tervezési fázisban feltárunk olyan kockázatos lépéseket, amelyeket helyettesíthetünk kevésbé kockázatosokkal, akkor azt cseréljük le arra. Ezzel elkerültük a kockázatot. Az üzemelés során pedig kivezethetünk olyan szolgáltatásokat, amelyek kockázatosak.
- Fenntartás

  Születhet olyan döntés is, hogy nem reagálunk a várható veszélyekre. Ez nem azt jelenti, hogy nem foglalkozunk vele, csak nem hozunk ellenintézkedést. Ebben az esetben is számolni kell a kockázattal, például intézkedési terveket kell kidolgozni az esetleges bekövetkezéskor milyen reakció kell, hogy kövesse részünkről az eseményt. Itt állhat pénzügyi vagy egyéb más megfontolás is.

- Áthárítás

  A kockázat áthárításokat tipikusan szerződésekkel szokták megoldani, tipikusan akkor, amikor egy külső cégre hárítják át a felelőséget. Szerződésben kell rögzíteni például, hogy mit várunk el az adott szolgáltatótól, mennyi legyen a rendelkezésre állás az elektromos betáplálásnál, valamint mennyi kártérítés jár nekünk, ha ez nem teljesül. [109] [117]

4.5. DÖNTÉSTÁMOGATÓ RENDSZER

Neumann János már 1948-ban a Hixon Symposiumon tartott előadásában feltette a kérdést, amely a mai napig komoly kihívást okoz az informatikai rendszerek tervezését és üzemeltetetését végző személyek számára.

„Lehet-e megbízhatatlan szerkezeti elemekből megbízhatóan működő automatákat építeni?”

Forrás: [118] 50. o.

A Hixon Symposiumon tartott előadások leginkább a számítógépek megbízhatóságával foglalkoztak, de ma már a komplexebb rendszerekkel kapcsolatban még gyakrabban felmerülő kérdéssé vált. A számítógépeket felépítő elektronikai alkatrészek nem örök életűek és, bár statisztikai adatok a rendelkezésünkre állnak, de azt, hogy mikor melyik alkatrész fog meghibásodni nem tudhatjuk. A hibamentes működést elősegíthetjük az ideális közeli környezet kialakításával, a rendszer *„hibatűrő”* kialakításával, a folyamatok szabályozásával stb. Azt szokták vizsgálni, hogy egy rendszerelem meghibásodása, milyen hatással van a rendszer egészének működésére. Azonban ez egy kezdetleges számítógép esetében sem volt egyszerű, nemhogy egy adatközpont, vagy összekapcsolt adatközpontok esetében. Egy váratlan, vagy nem kívánt esemény hatásának csökkentése az ugyanolyan feladatot végző rendszerelemek párhuzamos üzemeltetésével, különböző technológiák, gyártók bevonásával, de független energia-szolgáltatókkal, telekommunikációs cégekkel történő szerződéssel is elősegíthető. Természetesen a költségek és az adminisztrációs többletfeladatok miatt mérlegelni kell, mikor éri ez meg. Hibás működésből adódó becsült veszteségnek és a befektetett költségnek összhangban kell lennie. A rendszerünknek robusztusnak és alkalmazkodónak kell lenni, csillapítva ezáltal a nem kívánt hatásokat. Ez azt jelenti, hogy a rendszer a hibákat részben elnyeli, vagy

késlelteti azok kimeneti hatását. Diverznek tekinthető a rendszerünk, ha a rendszerelemeket, bemeneti forrásokat, technológiákat párhuzamosan alkalmazzuk. [119] [120]

A természetben megfigyelhető jelenségeket, mint az öngyógyítást több dolog miatt is nehéz megvalósítani egy ember által épített és kézben tartott rendszernél. Egyrészt olyan mértékű túlbiztosításra és kapcsolati rendszerre lenne szükség, amely már túlzott mértékben megdrágítaná a rendszerünket, másrészt pedig folyamatos kontroll alatt akarjuk tartani a rendszerünket (legalábbis ma még ez a cél) és nem engedhetjük saját életet élni, illetve ma még nincs is rá módunk.

Véleményem szerint ma egyre inkább hangsúlyosabb Neumann megállapítása, amely azt mondja, hogy működésbiztonság szempontjából éppen olyan fontosak a szervezési kérdések, mint a technikai eszközök használata. Ezzel is igazoltnak látom a hipotéziseimben (H2, H3) állítottakat, miszerint szabályozott struktúra, illetve jogszabályozás (amely jelenleg hiányos) kell az üzemeltetéshez. [118] [121]

A szervezési és irányítási eszközöket segíti, ha a vállalatnál létrehozunk egy konfigurációkezelő rendszert. Az angol elnevezése többet mond, mint a magyar fordítás, így a továbbiakban az eredeti angol elnevezést a CMS-t használom. Az ITIL megfogalmazás szerint a CMS egy szoftver, amely képes kezelni az informatikai szolgáltatásokat biztosító komponensek és a közöttük lévő kapcsolatok konfigurációját. Magába foglalja továbbá az incidenskezelést, a problémamenedzsmentet, a tudásmenedzsmentet, a változáskövetést, az erőforrás- és dokumentumkezelést, valamint ezek kapcsolatrendszerének kezelését. Az alapadatok szintén tartalmazzák a rendszerrel kapcsolatba kerülő személyek, helyszínek, erőforrások, üzleti folyamatok és a környezet leírását. Azonban a CMS nem egyenlő a CMDB[130]-vel. A CMS része a CMDB. [122] [123]

Fontos tisztázni, hogy a CMDB nem váltható ki egy hálózat feltérképező alkalmazás [131] által biztosított adatbázissal. Hasonlóan nem keverhető össze a hálózatfelügyeleti- és rendszerfelügyeleti eszközök, szoftverek által szolgáltatott adatok nyilvántartása, tárolása. Ezek az alrendszerek a javasolt rendszerfelügyleti és beavatkozó rendszer részét kell, hogy képezzék, de nem válthatják ki egymást. A

[130] CMDB (Configuration Management DataBase) Konfiguráció Management Adatbázis
[131] Pl.: Nmap, NetCrunch stb.

rendszer részét kell, hogy képezze egy munkafolyamat leírás, amelyet a szolgáltatást biztosító személyek mindegyikének be kell tartani. A rendszerbe kerülő elemek adatait az egész életútjuk alatt nyilván kell tartani. [124] [125] [126]

Nagyon érdekes kérdés és problémakör, hogy egy rendszerelem (ITIL-ben konfigurációs elem[132]), mennyi tulajdonságát kell rögzíteni. Természetesen ennek meghatározása a rendszer kialakításakor kell, hogy megtörténjen. Mélységében és szélességében is vizsgálható a kérdés. Mélység alatt azt értem, hogy mennyire kell részleteiben vizsgálni egy eszközt. Például kell-e, tud-e hosszútávon információt adni egy routerben lévő kondenzátor, tekercs típusa, gyártmánya stb. Ezeket az adatokat, mint láthattuk a kockázatelemzésnél is fel kell használni. Érdekes azonban, hogy pont a kockázatelemzésből derülhet ki, hogy milyen adatokat kell nyilvántartanunk még. A szélesség alatt pedig azt értem, hogy milyen messze nyúl el a nyilvántartás keze. Szükséges-e nekünk az őrzésvédelmi rendszereket alkotó kamerák gyártó cégének tulajdonosi szerkezetét vizsgálni? [124] [125] [126]

A katasztrófavédelem honlapján olvasható az alábbi idézet, amely Bognár Balázs írásai között többször is megtalálható:

„A kritikus információs infrastruktúrát az alábbi öt fogalommal is jellemezhetjük:

- *kiemelt üzemeltetési eljárásmódok (központi irányítás és koordinálás);*
- *informatikai biztonság;*
- *dominóelv[133];*
- *leggyengébb láncszem és rész-egész elv;*
- *interdependencia[134].”*

Forrás: [127]

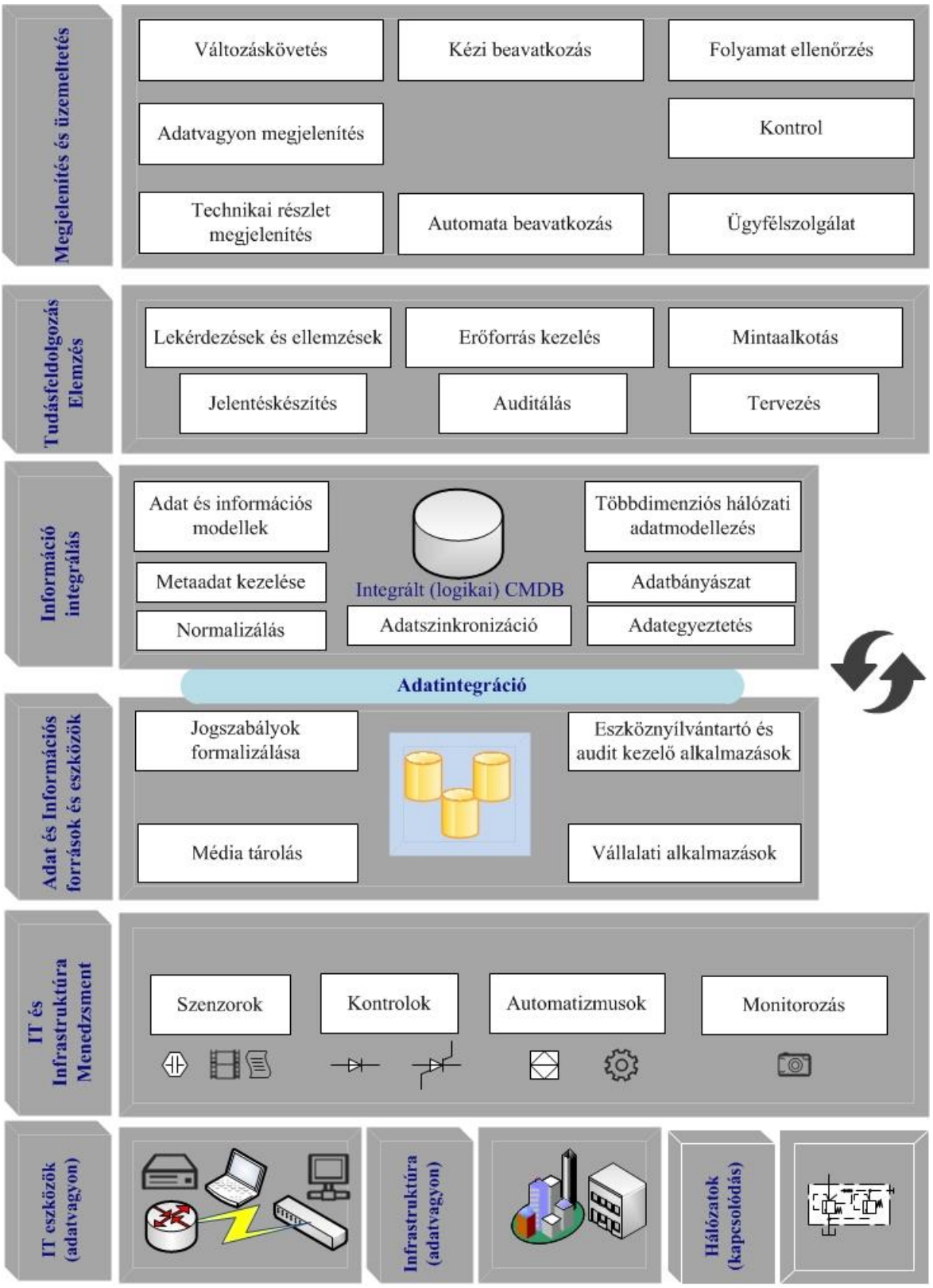
A felsorolásban megtalálható az egymástól való függőség, a leggyengébb láncszem és rész-egész elv, valamint a dominó elv, melyek vizsgálatához a hálózatelméleti tudomány nagy segítséget nyújthat. Véleményem szerint egy megfelelő szoftver kiválasztásával, amely a hálózatelméleti algoritmusokat használja fel a működése során, nagyban növelhető lenne a kritikus információs infrastruktúra biztonsága. A üzemeltetési eljárásmódok pedig az ebből kinyert információk alapján

[132] Komponens, amelyiket felügyelni kell valamilyen IT-szolgáltatás nyújtása érdekében.
[133] Láncreakciószerű sérülés/károsodás.
[134] Interdependencia egymástól való függőség

tökélesíthetőek lennének. Minél nagyobb és kritikusabb [135] egy informatikai infrastruktúra annál bonyolultabb, komplexebb felépítésű és annál nehezebb az üzemeltetés számára egy CMS segítsége nélkül átlátni az egész működését. A rendszerelemek bonyolult kapcsolatai eredményezhetnek olyan nem várt esemény bekövetkezését, amely negatív irányba mozdíthatja el a rendszer működését.

Kiegészítve az ITIL-ben lévő CMS-t (lásd: 9. számú melléklet), a következő kialakítást tartom a legjobb megoldásnak.

[135] Kritikusabb alatt azt értem, hogy az üzemszerű és elvárt működéstől való eltérés veszélyeztetheti más rendszerek, emberek, közösségek életminőségét.



10. ábra Felügyeleti és beavatkozó rendszer a CMS alapján
(saját szerkesztés az ITIL alapján [210]*)*

A legalsó szinten helyezkednek el az informatika, a hozzátartozó (épület elektronikus berendezései, klíma, UPS, beléptető és riasztó rendszer, tűzérzékelő és oltórendszer, zártláncú videó hálózat stb.) infrastruktúra elemei és az őket összekötő fizikai hálózati kapcsolatok. Ez a szint minden esetben megvalósul, még ha hiányosan is, mert különben nem is létezne informatikai rendszer. [124]

A következő szinten az érzékelők helyezkednek el. Itt találhatóak meg a rendszereket – általában a gyártó által szállított – vezérlő eszközök, szoftverek. Léteznek integrált rendszerek is, ilyenek például azok a biztonsági rendszerek, amelyek egy egységet képeznek a beépített beléptető, riasztó, zártláncú videó és tűz jelző rendszerek által. Ezek kimenete sokszor az IT rendszer bemenete is lehet, amikor például a tűz, vízbetörés esetén utasítják az IT infrastruktúrát a rendszer mentésére, leállítására. Ezen a szinten már információs infrastruktúráról beszélünk, mert az infrastrukturális elemeket komplexen kezeljük. [124]

A következő szinten jelennek meg a rendszerenként különálló CMDB-k, vagy a dokumentum könyvtárak. A szenzorokból érkező jeleket átalakítást követően az adatbázisban tároljuk. Itt nagy a felelőssége a tervezőnek, mert nem adatokra, hanem információkra van szükségünk. Ezt azonban gyakran a nagyon sok adatból nem lehet kihámozni, a nagyon kevés adat pedig téves információkat adhat. [124]

Az integrációs szinten jelenik meg az egységes CMDB. Ez lehet valóban egy önálló adatbázis, de hasznosabb, ha virtuális értelemben jelenik meg egy adatbázisban. Ahhoz, hogy a különböző adatbázisok adatait egységként kezeljük szükséges például az adatok metaadatait központilag menedzselni, elvégezni a szükséges átalakításokat, megtalálni és nyilvántartani a közös pontokat. Természetesen a szinkronizáció ütemezése és végrehajtása az egyik legkomolyabb feladat ezen a szinten. [124] Ezen a szinten lehetséges összekötni a különböző hálózatokat. Ezt megtehetjük mi is, de a következő szinten a rendszer javaslatot tesz, illetve automatikusan össze is kötheti az egyes hálózati csomópontokat. Ilyen lehet például a router, mint hálózati elem és a kezelője, akinek jogosultsága van hozzáférni ahhoz, de ilyen lehet az egy helyen elhelyezett klíma, szerver és tűzoltó berendezés stb. Ezek általában nincsenek egy adatbázisban, de a többdimenziós összeköttetéssel új megvilágításba kerülnek. A gráfelméletben bemutatott *2*. ábra és 3. ábra ezeket a kapcsolódásokat mutatja be. A javasolt döntéstámogató rendszer újdonsága és fő haszna abból adódik, hogy egyrészt az ábrán látható részegységek egy egészként működnek, másrészt a párosgráf és a

többdimenziós matematikai elméleti tudást, beépül az integrációs és a tudásfeldolgozó, elemző szintbe. Ezzel egy dinamikus elemzés hajtható végre a különböző hálózati szinten megjelenő hálózati elemek közt, így már nem csak beszélnek róla, hogy egy komplex védelmet kell nyújtani a rendszernek, hanem technikai megvalósulás is megtörténik. A rendszer tökéletes működéséhet szükséges alkalmazott matematikai módszerek, algoritmusok kidolgozása és programozó matematikusok által megírt kódok.

Amennyiben rendelkezésünkre áll a tömeges adat, akkor a tudásbázis szinten kezelhetjük azokat. Itt nem csak az aktuális adatokat, de az archiváltakat is hasznosítani lehet, illetve kell. Itt valósulnak meg a különböző elemzések (például kockázatelemzések), lekérdezések, a mintaalkotások, amelyek segítségével algoritmusokat hozhatunk létre. A 2. fejezetben említett algoritmusok, mátrix számítások ezen a szinten valósulnak meg. Az adatok halmaza, azok kapcsolódása, időbeni változása olyan összefüggéseket mutathat, amelyet külön-külön nem vehetnénk észre. A rendszer jelzési és riasztási eseményeit komplexen lehet kezelni, amely hatékonyabb beavatkozáshoz vezethet. [124]

A legfelső rész gyakorlatilag a rendszerfelügyeleti szint, a jelzéseket, elemzéseket megtekinthetjük, az üzemeltető személyzet utasításokat adhat ki. Ez a szint biztosítja a felső vezetés részére is az információ megjelenítést. A felügyeleti rendszer a tudásbázis által biztosított algoritmusok és az adatbázis adatai segítségével automatizmusok segítségével javaslatokat tehet a beavatkozásra, vagy akár automatikusan végre is hajthatja azokat. [124]

Abban az esetben, ha külső információáramlás is szükséges, akkor ellenőrzött formában becsatlakozhat különböző szinteken is az együttműködő szervezet. A maximális biztonságot is szem előtt tartva a kapcsolat egyirányú kell, hogy legyen, és a kimenő adat az ellenőrzést követően adatdióda[136] segítségével továbbítható. [124]

A rendszer kiépítettségét tekintve, egy cég különböző fejlettségi szinten lehet. A moduláris felépítés miatt lehetőség van szakaszosan végrehajtani kiépítést. Az egyik legkritikusabb rész egy már működő cég esetében az adatbázisok integrációja, a közös CMDB létrehozása. A CMDB-t tekintve is több fejlettségi mutató lehet, amelyek a következők:

[136] Adatforgalom egy irányra korlátozását kikényszerítő eszköz. A segítségével a magasabb minősítésű vagy védettebb hálózatból nem kerülhet át adat egy alacsonyabb szintűbe, csak az alacsonyabból a magasabba.

- Az információk a rendszerről többnyire a közvetlen üzemeltető állomány fejében léteznek. Legtöbbször a tudás hatalom elv alapján nem osztják meg az információt mással, így vélik biztosítottnak a munkahely megmaradását, a nélkülözhetetlenséget.
- Valaki leírja saját Word, Excel dokumentumba, jobb esetben valamilyen adatbázisba a saját számítógépén. Ez azonban egy bonyolultabb rendszernél már nem valósítható meg, mert az hamar a rendszer összeomlásához vezetne.
- Az előbb létrehozott nyilvántartásokat közös mappákban tárolják. Ebben az esetben, ha az üzemeltető személlyel történik valami, van esély a leírás megtalálására.
- Ezen a szinten már a közös mappában tárolást valamilyen szabály írja elő, így a mapparendszer is előre kidolgozott, átlátható. Így valóban kezelhető az információ abban az esetben is, amennyiben kiesik a rendszert alkotó személy.
- Egy magasabb fejlettségi szint, amikor már adatbázisban tárolják az adatokat. Így az adatok gyorsan kezelhetők, azokkal könnyebb feladatokat végrehajtani.
- A következő szint, amikkor az összes információt egy fizikai vagy virtuális adatbázisban tárolunk, amely természetesen szabályozott módon történik.
- A legfejlettebb, amikor a cég normál működése során már nem is lehet végigvinni egy folyamatot a CMDB használata nélkül. [124]

Nagyon kritikus pontja a rendszernek a változáskövetés. Minden rendszerben a változások kockázatokat hordoznak magukban, tehát kiemelt figyelmet igényelnek. Végig kell menni a jóváhagyási fázisokon és ha szükséges lehetőséget kell biztosítani a visszaállásra is. Fontos tényező, hogy a rendszerünkben nem statikus adatokat kell tárolni, hanem az aktuálisakat és a múltbelieket egyaránt, tehát a változásoknál minden esetben el kell tárolni mindkét információt.

Véleményem szerint egy kritikus információs infrastruktúrát üzemeltető cégnél szükséges a legmagasabb szintet elérni. Ezek a rendszerek már annyira bonyolultak, hogy másképpen nem tartható kézben a biztonságos üzemeltetés.

A másik fontos szempont, hogy a kezelő személyektől nem függhet közvetlenül az infrastruktúra működése. A személyzet cserélődése nem okozhat fennakadást. Az információ minden esetben rendelkezésre kell, hogy álljon az új szakembereknek is a lehető legrövidebb időn belül. Persze nagyon nehezen helyettesíthető az a karbantartó, aki az iskola elvégzését követően már a cégnél dolgozott és most készül nyugdíjba menni, de egyszer mindenki el fog menni a cégtől. Amennyiben a cég rendelkezik a legfelső szintű logikus felépítéssel, a „szervezési" eszközökkel viszonylag könnyen megvalósítható a rendszer passzív állapota[137]. A közös kezelőfelületbe folyamatosan integrálhatók a gyártók által szállított kezelőfelületek. Persze itt is van egy nagy kérdés. A gyártók rendelkezésre bocsátanak-e minden információt, biztosítják-e a megfelelő csatolófelületet az információáramláshoz. Üzemeltetés szempontjából nagy előnyt jelenthet egy homogén rendszer kialakítása, az azonos gyártók kiválasztása. Ez azonban ellentmondásban van azzal, hogy a magas rendelkezésre állás különböző technológiák, gyártók alkalmazását követeli meg. [124] [128]

Az egyik legfontosabb rendszerelem az ember, amelyről jelenleg a CMS rendszerek nagyon kevés információt tárolnak. Ráadásul ezeket az adatokat teljesen más módszerrel kell felvinni a CMDB-be, mint a rendszerek adatait. [124]

A felhasználók viselkedésének rögzítésére már ma is rengeteg eszköz áll a rendelkezésünkre, de léteznek olyanok is, amelyek a személy együttműködése nélkül is összegyűjtik a kívánt információkat, ilyen pl. a viselkedés alapú profilkészítés. Persze ezek számos etikai és jogi kérdést is felvetnek, de létezhet olyan környezet, ahol ezzel együtt kell élni. A hétköznapokban is megfigyelnek ilyen eszközökkel minket, például amikor az internetet használjuk, majd ezeket az adatokat kereskedelmi céllal fel is használják. Lépten-nyomon otthagyjuk a digitális lenyomatunkat mindenhol, ahol az informatikai eszközök által kezelt rendszereket használjuk. Érdekes adat az internet használatakor, hol mennyit időztünk, milyen billentyűzet vagy egér aktivitásunk van, honnan jöttünk és merre tartunk. Talán mégis a legveszélyesebbek a felhőben tárolt adatok. Sajnos sok cég az ügyfelek adatait tárolja üzletileg egyes esetekben talán valóban a leghatékonyabban egy harmadik fel által biztosított szolgáltatásként, a virtuális IT környezetben. Az embereknek általában az a normális viselkedése, hogy követni akarják a társadalmi normákat, a csoportok viselkedését, és a legtöbben feljebb

[137] Passzív alatt azt értem, hogy a rendszer nem képes automatikusan beavatkozni a működésébe. A kezelőszemélyzet egy rendszert használ, jogosultsági szintnek megfelelő lekérdezéseket tudnak végrehajtani és utasításokkal vezérlik a rendszert.

és feljebb akarnak kerülni ranglétrákon, vagy meg akarnak felelni a cégüknek, főnöküknek. Ezektől a viselkedési formáktól a környezeti változás fogja őket eltéríteni. A rendszerünk viselkedésének megjóslásánál az emberi tényezők mellett, amelyek sokszor kiszámíthatatlanok, a gyártók megadnak az alkatrészek, eszközök tekintetében olyan adatokat, amely a meghibásodási valószínűséget mutatják. Ezeket az adatokat is bevihetjük az adatbázisunkba, így a gráfelméletben alkalmazott algoritmusok segítségével olyan elemzéseket végezhetünk, amik a rendszer nagyobb megbízhatóságát segítik elő. [124]

De ezeket az adatbázisokat összekötve egy cég biztonsági rendszerével, mozgásnaplónkkal és kapcsolati hálónkkal még értékesebb információt kapunk. Főleg, ha nem csak az aktuális adatokat figyeljük, hanem tendenciákat és összefüggéseket is keresünk. Ezzel is bizonyítottnak látom a többdimenziós hálózatok kapcsolatát elemzését (H1), amely a felsorolt adatbázisokból épülne fel.

A kérdés, hogy mikor kapcsoljuk ezeket mind össze, illetve mikor leszünk képesek kezelni az óriási mennyiségű adatot. Véleményem szerint nem a biztonsági terület lesz az, ahol elsőként hasznosítják az elméletben elért eredményeket. Az üzleti életben a potenciális vásárlók felkutatására és a reklámok célba juttatására is hatékony módszer lehet, ezért már ma is rengeteg pénzt fordítanak rá, és később az emberekkel is elfogadtatják a kellemetlen oldalát is. [129]

Természetesen az adatok gyűjtésével és elemzésével a gazdasági élet szereplői mellett, már ma is foglalkoznak a rendvédelmi szervek és titkosszolgálatok. Az első fejezetben bemutatott matematikai alapokkal, valamint a második és harmadik fejezetben lévő adatokkal véleményem szerint létrehozható egy olyan felügyeleti és beavatkozó rendszer, amely a kritikus információs infrastruktúra üzembiztoságából és informatikai biztonság szempontjából is hasznos lehet. Sajnos a kapcsolódások bonyolultsága és az adatok számossága nem segíti elő a robbanásszerű fejlődést, de talán a hálózatkutatásban elért eredmények segíthetnek ezen. Egy ilyen kutatási eredmény a nemrég megjelent publikáció is, amely Babai László[138] nevéhez kötődik, aki egy új eljárást mutatott be, ahol egy algoritmus segítségével gyorsabban megállapítható két gráf azonossága. Ez segítséget nyújthat az informatikai rendszerek felügyeleténél, persze akkor, ha megfelelő számú információ áll a rendelkezésünkre. [130]

[138] Babai László (1950 -) matematikus, Chicagói Egyetem oktatója.

Hasznos lehet például, ha a mintákat, az előzményeket összehasonlítjuk az aktuális helyzettel. A módszer tűzfalak esetében már ma is egy létező gyakorlati alkalmazás, de a komplex rendszerek esetében még nem. **A hipotézisemben (H4) vélelmeztem, hogy egy CMS-el kiegészített rendszerrel magasabb fejlettségi szintre hozható a kritikus információs infrastruktúra. Az értekezésemben bemutatott rendszer véleményem szerint alkalmas lehet erre a célra.** A rendszer használatához, mint az időjárás előrejelzés esetében is sok adatra van szükség, és minél későbbi bekövetkezendő eseményt akarunk előre jelezni, a megbízhatósága annál bizonytalanabb lesz. Egy nem várt eseménynél a reagáláshoz az üzemeltető személyzetnek a lehető legtöbb időre van szüksége, hogy biztosítsa az üzletmenet folytonosságot az informatikai rendszerek segítségével. Sajnos azonban ma a legtöbb védelmi és a riasztást kiváltó eszköz már csak az esemény bekövetkezésekor jelez, amikor azonnal reagálni kell. [131]

Egy Gartner felmérésében 18 adatközpontok infrastruktúrakezelő[139] szoftvert hasonlítottak össze. Ezek közül néhány: Nlyte Software, Schneider Electric, Sunbird Software, Vertiv, CommScope, FNT stb. [132]

„Az adatközpontok infrastruktúrakezelő (DCIM) eszközei felügyelik, mérik, kezelik és / vagy irányítják az adatközpontok erőforrásait és az energiafogyasztást, amely magába foglalja mind az IT-eszközöket (például szerverek, tárolók és hálózati berendezések), mind a kiszolgáló berendezéseket." [132] (saját fordítás)

A felsorolt szoftverek közül részletesebben tanulmányoztam a Schneider Electric, Sunbird Software, valamint a listában nem szereplő HPE Operations Orchestration alkalmazásokat. Az általam javasolt megoldás előnye, hogy a moduláris felépítés, valamint a CMS alap miatt jobban illeszkedik a kritikus információs infrastruktúrához, amelyet központilag ütemezetten lehetne bevezetni. Az egységes szoftverrel gazdaságosabb és hatékonyabb üzemeltetés érhető el. [119] [120] [133]

4.6. ÖSSZEGZÉS

Neumann János megállapítása, amikor a szervezési eszközöket említi mindenképpen igaz a kritikus információs infrastruktúra esetében is. Azt, hogy a szűk reagálási időt, hogyan használjuk ki, azt az előre megtervezett intézkedési stratégiákkal

[139] DCIM (Data Center Infrastructure Management) Adatközpont infrastruktúrakezelő

lehet a leghatékonyabbá tenni, és egy komplex rendszerre kidolgozott biztonsági, üzemeltetési utasítással, rendszabállyal lehet a bekövetkezés előtt megnövelni a várható időkeretünket. A felügyeleti és beavatkozó rendszer, amelyben rendszerezett formában gyűjtjük az adatokat, elősegíti az átláthatóságot és egyes esetekben az automatizmussal csökkenti a reagálási időt is. A rendszer úgy működik, mint a Neumann elv. A tárolt adatokon (CMS) az előre megírt vagy a folyamatában kidolgozott program (matematikai alapok, hálózatelmélet stb.) elvégzi a műveleteket.

A technikai fejlődés és a jelentős költségfelhasználás miatt az informatika egyre inkább a cégvezetők és a gazdasági vezetők figyelmének középpontjába kerül. Az informatikai rendszer üzemeltetésével kapcsolatban két szélsőséges lehetőség között kell vállasztani egy vezetőnek. Az egyik véglet az erőd módszer, amikor olyan rendszert épít, melynek teljesítménye, biztonsága többszöröse a szükségesnél[140]. A másik véglet, amikor nem foglalkozik az esetleges veszélyforrásokkal, eleve számít rá. Ez utóbbi megoldás biztosan nem lehet opció egy kritikus információs infrastruktúra esetében. A jó megoldás az optimális állapot megtalálása.

Ennek érdekében a hipotézisem szerint (H4) szükséges egy centralizált menedzsment szoftver, amely az egész rendszert kézben tartja és azt egy IT szervezet üzemeltet. Természetesen a speciális szoftvereket a megfelelő személyzet kezeli, pl. őrség, biztonsági szervezet stb. A kutatásom során a szakirodalom feldolgozását követően több informatikai rendszert üzemeltető szervezet vezetőjével konzultáltam és megbizonyosodtam arról, hogy feltevésem időszerű és szükséges.

Véleményem szerint kiemelten fontos a program és a kritikus információs infrastruktúra pontos megtervezése, előkészítése, a kapcsolódási pontok helyes megválasztása, dokumentáltsága, a rendszer kiszámíthatósága. A tervezés és üzemeltetés is egyszerre statikus és dinamikus. Egy adott időpillanatban detektáljuk a jelet, a viselkedést, ami azonban a következő pillanatban már változik. A változás iránya, dinamikája is érdekes lehet egy adott folyamat tekintetében.

Az automatikus beavatkozó rendszer létrehozatalakor fontos szem előtt tartani azt is, hogy bármikor szükség lehet egy emberi beavatkozásra alkalmas kicsatolásra is, amellyel felülbírálható a döntésmechanizmus, visszaállhatunk egy korábbi verzióra. Másik tény, amit figyelembe kell venni, hogy a hálózat a véletlen hibákkal szemben akkor védett, ha rendszerszemlélet figyelembe vételével építjük azt és nem

[140] Pl. otthoni használatra atomerőművekben alkalmazott eljárások, eszközök vannak.

véletlenszerűen [141] alkotják a rendszert a rendszerelemek. Igaz, ekkor ezekben a skálafüggetlen hálózatokban a direkt támadások veszélyesebbek. A kontrollált és lecsökkentett peremfelületeket, külső csatlakozási pontokat védve minimalizálható a támadások okozta kockázat. Csökkenteni kell tehát a véletlen események számát, hogy minimalizáljuk a pillangó effektus hatását. Véleményem szerint a gyakorlatban ez úgy érhető el, hogy erősen szabályozzuk a rendszert, valamint a környezetét és törekszünk a stabil állapot fenntartására. Ha valami eltér a normálistól, akkor azt vissza kell kényszeríteni, egyébként az egymásra gyakorolt hatások káoszt eredményeznek. Az, hogy mi a normális állapot pontosan definiálni kell. A felügyeleti és beavatkozó rendszer folyamatosan kalkulációt készít (például hálózatelméleti alapon) arról, hogy éppen akkor mennyi a valószínűsége egy másik állapotba való átlépésre. A rendszert fel kell készíteni a szigetszerű üzemeltetésre, amikor bizonyos részeit lekapcsoljuk a kritikus információs infrastruktúrának. Az új rendszernek el kell látni a felügyeleti és beavatkozó funkciókat, továbbá fel kell használni az adatvagyon és a többdimenziós hálózati gondolkodásmód mellett a szeparált felügyeleti rendszerek adatait is.

[141] Véletlenszerűség: éppen milyen szoftver vagy hardver van priorizálva a különböző indokok miatt, vagy dömpingszerű, ad-hock fejlesztések vannak.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Az értekezésem egyik kulcs mondanivalója, hogy a biztonságos üzemeltetést hálózatelméleti, azaz rendszerszemléletű megközelítéssel kell kezelni, a rendszerünknek folyamatosan, kontroláltan és stabilan kell üzemelni.

A technológia fejlődése, a globalizmus és az embereknek a géptől való függése mind hozzájárul ahhoz, hogy a rendszerek egyre bonyolultabbak lesznek és már-már úgy tűnik kezelhetetlennek. Ezzel magyarázható Eric Emerson Schmidt mondása is, amit az értekezésem elején már idéztem.

„Az Internet az első dolog, amit az ember épített, s amit mégsem ért. Ez a valaha volt legnagyobb kísérlet az anarchiára.”

Forrás: [2]

Ez a jelenség figyelhető meg számos nagy rendszernél és ezt az anarchiát kell elkerülni a kritikus információs infrastruktúra esetében. A hipotézisek, amelyeket állítottam a kutatásom megkezdésekor azt a célt szolgálják, hogy egy rendszert csak rendszerszerű gondolkodással lehet üzemeltetni. A szakirodalom feldolgozása és a konzultációk bebizonyították számomra, hogy a hipotéziseimben állítottak helytállóak. Egy erősen szabályozott üzemeltetési környezetet kell létrehozni annak érdekében, hogy kézben tarthassuk a kritikus információs infrastruktúra üzemeltetését. A rendszernek minden körülmények között a normál állapotban kell működnie, kerülve a káoszt. Ehhez szükségesek az adminisztratív feltételek, például törvényi megfelelés, szervezeti és munkafolyamat struktúra, valamint hálózatelméleti és egyéb matematikai alapokon nyugvó informatikai támogatás.

A biztonságos rendszer megteremtéséhez nem elég a rendszer egyes elemeit biztonságossá tenni, nem elég szoftvereket alkalmazni, amelyekkel detektálhatók vagy megelőzhetők az incidensek, hanem a rendszerünket egy komplex egészként kell értelmezni. Az üzemeltető és felhasználó személyek, a folyamatok összessége, a jogszabályok és maga a rendszer kölcsönhatásban vannak egymással. Ezeket folyamatosan karban kell tartani és biztosítani kell a működéséhez szükséges feltételeket.

A szakembereket folyamatosan magas szinten kell, kellene képezni, konferenciákra, kiállításokra utaztatni annak érdekében, hogy a kor színvonalát képviselő technikát, technológiát legyenek képesek üzemeltetni. Ez különösen költséges, ha az állami szférában működő kritikus infrastruktúrát üzemeltető

szervezetek különböző típusú szoftver és hardverelemeket használnak. Meggyőződésem, ha központi irányítás alá vennék ezt a területet jelentősen csökkenthetők lennének a költségek. Az egyetemekkel kötött megállapodásokkal specifikus képzéseket lehetne indítani, vagy az adott szoftver oktatási licenszét megvásárolva ingyenes oktatással folyamatosan magas szinten lehetne tartani az üzemeltető állomány tudását.

A jogalkotásnak, rendeleteknek és szabályozásnak összhangban kell lenni országon belül és meg kell teremteni a jogharmonizációt legalább a szövetséges országok tekintetében. EU szinten elkezdődött már az egységes kezelése a területnek, ennek köszönhetően jött létre a 2016/1148 irányelv is.

Amennyiben egy törvény kimondja, hogy a kritikus infrastruktúrát üzemeltet egy szervezet az ország érdekében, akkor nem szabad belső vagy bármilyen szabályzókkal annak feltételeit ellehetetleníteni. Egy ellentmondás keletkezik, amely egy kritikus infrastruktúra üzemeltetése során minden esetben veszélyes. Még egy alacsony szintű vagy sok egyenként elhanyagolható kockázat sem engedhető meg egy kritikus infrastruktúránál, még akkor sem, ha a vezetés tudtában van és felvállalja ennek következményét, mert önmagával kerül ellentétbe a kritikus infrastruktúra. Ekkor ugyanis véleményem szerint nem értelmezhető a „kritikus" infrastruktúra. Amennyiben nem tartom annyira fontosnak, hogy a feltételeket is biztosítsam a megfelelő színvonalon, akkor az nem lehet kritikus. Fontos feltárni a kritikus infrastruktúrák közötti kapcsolatokat, vizsgálni kell az interdependenciát, amely a rendszerek kölcsönös egymásra hatását jelenti. Ezeket a hatásokat is mérni és elemezni kell, illetve az eredmények alapján fel kell készülni az ebből eredő veszélyek elhárítására. A különböző rendszerek egymásra gyakorolt hatásai felerősíthetik az önmagukban elhanyagolható veszélyeket. A kialakult hidak belengéseket idézhetnek elő, illetve rejtett átjárók keletkezhetnek.

A kialakítandó döntéstámogató rendszernek fel kell használni az adatvagyon és a többdimenziós hálózati gondolkodásmód mellett a szeparált felügyeleti rendszerek adatait is. A rendszer fejlesztését állami szinten képzelem el, például egyetemi pályázatokkal.

A kutatásom során az induktív és deduktív kutatási módszerek segítségével bebizonyosodott számomra, hogy az értekezésem elején megfogalmazott hipotéziseim helytállóak.

Új tudományos eredmények

1) Hálózat, rendszer, üzemeltetés biztonság és a kritikus informatikai rendszer definíciójának megalkotása.

Definiáltam mit jelent a hálózat, rendszer és az üzemeltetés biztonság amennyiben ezeket a fogalmakat a kritikus informatikai infrastruktúra kapcsán említjük. A hálózat és rendszer definíciója pontosan meghatározza az értelmezési tartományt, amelyben üzemeltetni kell. Az üzemeltetés biztonság pedig definiálja, mi a legfontosabb cél az üzemeltetés számára a biztonság betartása mellett. Az előzőek alapján pedig meghatároztam mi a kritikus informatikai rendszer.

2) Értekezésemben rámutattam az ember-technika-környezet interdependenciájára, ami alapján kimondható, hogy a többdimenziós hálózatelméleti alapok alkalmazásának bevezetése a rendszerszemléletű gondolkodással elősegítheti a biztonságosabb és komplexebb informatikai rendszerüzemeltetést.

Amennyiben a különböző hálózatokat egy szintnek, egy hálózati rétegnek tekintjük, létezik az emberek kapcsolatrendszerét leíró réteg, a technikai eszközöket ábrázoló rétegek (fizikai kábelezések, logikai kapcsolatok az informatikai rendszerek közt, elhelyezkedésük szerinti stb.) az adatkapcsolati réteg, a jogszabályi struktúra alkotta hálózatok stb. Ezeket a rétegeket külön-külön vizsgálva eltérő eredményt kaphatunk, mintha a köztük lévő kapcsolatokat feltérképezve együtt vizsgálnánk az egészet. Későbbi kutatásokkal, algoritmusok kidolgozásával és ezek alkalmazásokba történő implementálásával elősegíthető egy üzembiztosabb informatikai üzemeltetés.

3) A kritikus információs infrastruktúra üzemeltetéshez szigorúan szabályozott struktúrát kell kiépíteni, mind a szervezeti felépítésben, mind a környezeti jogszabályok területén és az informatikai rendszerünket kiszolgáló infrastruktúrában.

A kiépítésnek hierarchikus, felülről szerveződőnek kell lennie. A kiépítést a kormányzati szintről kell kezdeni. A kialakított struktúrával csökkenthető a kockázata annak, hogy a skálafüggetlen hálózatoknál tapasztalható, egy hálózati elem gyengesége okozta meghibásodás, az egész hálózat működésére hatással legyen. A másik fontos oka a szabályozásnak a káosz elkerülése, amely a normál és a katasztrófa közti állapotot

jelenti. A felülről szerveződött hierarchikus felépítéssel, a központosított oktatási rendszerrel, szoftvergazdálkodással stb. költségtakarékosabb működés érhető el.

4) Rámutattam, hogy jelenleg Magyarországon a kritikus informatikai rendszerek üzemeltetéséhez szükséges jogszabályi hátterek hiányosak.

A homogén, hierarchikusan felépülő jogszabályi rendszerrel biztosítható, hogy a kritikus információs infrastruktúrák Magyarországon egységes rendszerként kezeljük. A szabályzókba be kell építeni a szabványokat, ugyanakkor egyes szabványok betartatását jogszabályokban kell elrendelni. Az egységes kezelés érdekében a törvény erejénél fogva létre kell hozni a Nemzeti Létfontosságú Információs Rendszer Üzemeltetést Koordináló Testületet, a Stratégiai Kutatóintézetet, kialakítani az oktatási rendszert és egy szervezetet, amely a magas szintű informatikai támogatásra képes.

5) Felvázoltam egy felügyeleti és automatikusan beavatkozni képes rendszer felépítésének egy lehetséges módját.

A döntéstámogató rendszer egységesen kezeli a szenzorok jelétől kezdve a megjelenítő rétegig minden egyes rendszerelem működését. A rendszer alapja a konfigurációs adatbázis, amelyben lévő adatokon végezhető el a különböző vizsgálat. A többdimenziós hálózati modell alkalmazása az információ integrációs és a tudásfeldolgozó elemző rétegben elősegíti a komplex rendszerelemzést. A dinamikus elemzés összehasonlításokat végezhet a múltbeli pillanatképek és a jelenlegi helyzetekkel, ami alapján eseményeket generálhat a rendszer. A jövőben elméleti és alkalmazott matematika módszerekkel továbbfejleszthető a rendszer.

Ajánlások

Az értekezésem tudományos eredményeit a részletes kidolgozást követően, elsősorban az állam által közvetlen, vagy közvetett módon a kritikus információs infrastruktúra üzemeltetés területén képzelem el hasznosítani. Mint korábban említettem ezzel költségek takaríthatók meg és az üzemeltetés biztonság jelentősen javítható.

A javasolt rendszer stabil működése kizárólag gondos tervezéssel érhető el és építőelemenként kell bevezetni. Kezdetben kisebb szervezetekre kell kiépíteni, majd kiterjeszteni egyre nagyobbakra, tehát egy alulról induló építkezést javaslok.

Az adminisztratív témaköröket tekintve (jogszabályok, struktúra kialakítása) az előzőekkel ellentétben a felülről lefelé történő kiépítés az indokolt.

HIVATKOZOTT IRODALOM

[1] **Kovács László**, Kritikus információs infrastruktúrák Magyarországon, Robothadviselés 7. Tudományos Szakmai Konferencia, 2007. november 27. Elérhető:http://hadmernok.hu/kulonszamok/robothadviseles7/kovacs_rw7.html#9. [Hozzáférés dátuma: 2017.03.31.].

[2] **Schmidt Eric Emerson**, Elérhető: http://www.citatum.hu/idezet/39268. [Hozzáférés dátuma: 2017.03.31.].

[3] **Beleznay Péter**, *szerző*, Az Internet története, Networkshop 2012 konferencia, Nemzeti Információs Infrastruktúra Fejlesztési Intézet, Elérhető: http://niif.videotorium.hu/hu/recordings/4081/az-internet-tortenete. [Hozzáférés dátuma: 2017.03.31.].

[4] **Georgi Dalakov,** Paul Baran, Elérhető: http://history-computer.com/Internet/Birth/Baran.html [Hozzáférés dátuma: 2017.03.31.].

[5] **Puskás Béla**, The risks of networks' complexity, Hadmérnök, pp. 167-171., 2012. VII. Évfolyam 4. szám, ISSN 1788-1919

[6] **Barabási Albert-László**, Behálózva, Budapest: Magyar könyvklub, 2003., ISBN 963-547-895-x

[7] **Cambridge Computer Lab,** Introduction to Network Theory, Elérhető: https://www.cl.cam.ac.uk/teaching/1011/PrincComm/slides/graph_theory_1-11.pdf. [Hozzáférés dátuma: 2017.03.31.].

[8] **Munk Sándor**, Hálózatok fogalma, alapjai, Hadmernök, 2010. V. Évfolyam, 3. szám, ISSN 1788-1919

[9] **Haig Zsolt; Kovács László**, Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Tanulmány (TÁMOP 4.2.2/B-10/1-2010-0001), **Ványa László** (*szerkesztő)*, Budapest: Nemzeti Közszolgálati Egyetem, 2012.

[10] **Husi Géza**, Rendszerelmélet, Elérhető: http://old.eng.unideb.hu/vmt2/images/tantargyak/szimulacio/Rendszer%20szeml%C3%A9let.pdf. [Hozzáférés dátuma: 2017.03.31.].

[11] **Pokorádi László**, Rendszerek és folyamatok modellezése, Debrecen: Campus kiadó, 2008., ISBN 978-963-9822-06-1

[12] **A honvédelmi miniszter 39/2014. (V. 30.) HM utasítása** a Magyar Honvédség Informatikai Szabályzatának kiadásáról.

[13] **Puskás Béla**, Kritikus Információs Infrastruktúrák modellezése, Felderítő Szemle, 1. szám 13/3, pp. 95-107, 2014., HU ISSN 1588-242X

[14] **Ürmösi Károly**, A biztonság, a biztonság fogalma, Hadtudományi szemle, 6.4, pp. 147-154, 2013., HU ISSN 2060-0437

[15] **Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, Informatikai Tárcaközi,** Bizottság Informatikai rendszerek biztonsági követelményei 12. sz. ajánlás, Budapest, 1996.,
Elérhető: https://dsd.sztaki.hu/mockups/itb/ajanlasok/a12/index.html. [Hozzáférés dátuma: 2017.03.31.].

[16] **Munk Sándor**, Robothadviselés 7. Tudományos Szakmai Konferencia, 2007. november 27., Információbiztonság vs. Informatikai Biztonság, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest

[17] **Szenes Katalin**, (szerkesztő), Az informatikai biztonság kézikönyve Informatikai biztonsági tanácsadó A-tól Z-ig. (27. aktualizálás), Budapest,: Verlag-Dashöfer Szakkiadó, 2007. ISBN: 9639313122

[18] **2013. évi L. törvény** az állami és önkormányzati szervek elektronikus információbiztonságáról.

[19] **2009. évi CLV. törvény** a minősített adat védelméről.

[20] **AXELOS Ltd**., ITIL Foundation Course (FND02 v4.3),
Elérhető: http://www.itsmf.hu/documents/itil2modszertan_osszefoglalo_v3.1.pdf. [Hozzáférés dátuma: 2017.03.31.].

[21] **2080/2008. (VI. 30.) Korm. határozathoz tartozó Zöld könyv** a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról.

[22] **2012. évi CLXVI. törvény** a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[23] **Muha Lajos**, A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, Doktori (PhD) értekezés, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2007.

[24] **65/2013. (III. 8.) Korm. rendelet** a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

[25] **Dr.Haig Zsolt, Hajnal Béla, Dr. Kovács László, Dr. Muha Lajos, Sik Zoltán Nándor**, A kritikus információs infrastruktúrák meghatározásának módszertana, ENO Avisory Kft., 2009.
Elérhető: http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf. [Hozzáférés dátuma: 2017.03.31.]

[26] **Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége - Adatközpont- és Felhő Munkacsoport**,
Elérhető: http://ivsz.hu/wp-content/uploads/2015/09/IVSZ-adatkozpont-fogalomtar.pdf. [Hozzáférés dátuma: 2017.03.31.].

[27] **Kovács László**, Hálózatkutatás és szociolingvisztika, Magyar Nyelvőr. 135/1. 90-96., 2011. ISSN 1585-4515

[28] **David Rehak, Petr Novotny**, Bases for Modelling the Impacts of the Critical Infrastructure, 2016. Elérhető: http://www.aidic.it/cet/16/53/016.pdf. [Hozzáférés dátuma: 2017.03.31.].

[29] **Fazekas István**, Neurális hálózatok, Debrecen, Debreceni Egyetem Informatikai Kar, 2013. ISBN 978-88-95608-44-0

[30] **Vicsek Tamás**, A Magyar Tudományos Akadémia folyóirata,
Elérhető: http://www.matud.iif.hu/03mar/vicsek.html.
[Hozzáférés dátuma: 2017.03.31.].

[31] **Tél Tamás; Gruiz Márton**, Mi a káosz? (És mi nem az?), Fizikai Szemle 2005/6. 218.o., Fizikai szemle, Magyar fizikai folyóirat, 2005.
Elérhető: http://fizikaiszemle.hu/archivum/fsz0506/gruiz0506.html.
[Hozzáférés dátuma: 2017.03.31.].

[32] **MacKay David John Cameron**, CITATUM,
Elérhető: http://www.citatum.hu/idezet/63938. [Hozzáférés dátuma: 2017.03.31.].

[33] **Gerőcs László; Vancsó Ödön**, (szerkesztő), Matematika, Budapest: Akadémia Kiadó, 2010, pp. 1151-1224, ISBN 978 963 05 8488 3

[34] **Kátai Zoltán**, Gráfelméleti Algoritmusok, Kolozsvár: Scientia Kiadó, 2008., ISBN 978-973-7953-95-7

[35] **Takács Károly** (szerkesztő) **BCE Szociológia és Társadalompolitika Intézet**, Társadalmi kapcsolathálózatok elemzése, Elérhető: http://publikaciok.lib.uni-corvinus.hu/publikus/647793.pdf. [Hozzáférés dátuma: 2017.03.31.].

[36] **Fekete István, Hunyadvári László, Nagy Tibor, Giachetta Roberto, Bartha Dénes, Ilonczai Zsolt, Danyluk Tamás**, Algoritmusok és adatszerkezetek / Minimális költségű feszítőfák, Elérhető: http://tamop412.elte.hu/tananyagok/algoritmusok/lecke28_lap1.html. [Hozzáférés dátuma: 2017.03.31.].

[37] **Podobni Katalin**, Legrövidebb útkereső algoritmusok, diplomamunka, Budapest: Eötvös Lóránd Tudományegyetem Természettudományi kar Operációkutatási tanszék, 2009.

[38] **PlexMath**, MuxViz: visualization of multiplex networks, Elérhető: http://www.plexmath.eu/?page_id=327. [Hozzáférés dátuma: 2017.03.31.].

[39] **Albert Solé-Ribalta, Clara Granell, Sergio Gómez and Alex Arenas**, Information transfer in community structured multiplex networks, Elérhető: http://journal.frontiersin.org/article/10.3389/fphy.2015.00061/full. [Hozzáférés dátuma: 2017.03.31.].

[40] **Vicsek Tamás, Szabados László** (szerkesztő), Hálózatok, Budapest, A Magyar Tudományos Akadémia folyóira. 167. évfolyam – 2006/11. szám, ISSN 0025 0325

[41] **Puskás Béla**, Hálózatelméleti alapok, 2012., Elérhető: http://www.puskashirbaje.hu/index_htm_files/Puskas_Bela_Halozatelmeleti_alapok.pdf, [Hozzáférés dátuma: 2017.03.31.].

[42] **Kormányzati Eseménykezelő Központ (GovCERT-Hungary)**, Spamhaus stílusú DDoS, Elérhető: http://tech.cert-hungary.hu/taxonomy/term/3576. [Hozzáférés dátuma: 2017.03.31.].

[43] **Csermely Péter**, A rejtett hálózatok ereje, Budapest: Vince kiadó, 2005. ISBN 963 9552 64 X

[44] **Kürtös Zsófia**, A társadalmi kapcsolatháló elemzés módszertani alapjai, Letenyei László (szerkesztő), Településkutatás szöveggyűjtemény, Budapest: Ráció, pp. 663-685.

[45] **Puskás Béla**, Kritikus információs infrastruktúrák biztonsága, sérülékenysége, Szakmai szemle, pp. 126-149, 2013., HU ISSN 1785-118

[46] **Székely Balázs**, Markov-láncok, Elérhető: http://www.math.bme.hu/~szbalazs/oktatas/sztoch_info/het_4_Markov.pdf. [Hozzáférés dátuma: 2017.03.31.].

[47] **Symantec**, Internet Security Threat Report, Elérhető: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. [Hozzáférés dátuma: 2017.03.31.].

[48] **Bodnár Balá**zs, A Magyar Köztársaság védelmi igazgatási rendszerének lehetséges korszerűsítése - Doktori értekezés, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem Kossuth Lajos Hadtudományi Kar Hadtudományi Doktori Iskola, 2009

[49] **Salamon Pál**, A Sorel-ház, Pécs: Alexandra, 2010., ISBN: 9789632972398

[50] **Csernus Im**re, Bevállalja?, Budapest: HTSART, 2004., ISBN: 9632161572

[51] **Muha Lajos, Krasznay Csaba,** Az elektronikus információs rendszerek biztonságának menedzselése, Budapest: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, 2014., ISBN 978-615-5491-65-8

[52] **Szádeczky Tamás**, Szabályozott biztonság – Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan, doktori értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2011.

[53] **Puskás Béla**, Az informatikai rendszerek és a jogi környezet változásai, HÍRVILLÁM = SIGNAL BADGE, 2013. 4. évfolyam 2. szám, pp. 204-214, HU ISSN 2061-9499

[54] **A Katasztrófavédelmi Koordinációs Tárcaközi Bizottság 4/2016 határozata**

[55] **Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve** a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

[56] **Rossella Mattioli, Dr. Cédric Levy-Bencheton**, Methodologies for the identification of Critical Information Infrastructure assets and services, Elérhető: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport. [Hozzáférés dátuma: 2017.03.31.].

[57] **ENISA**, Gaps in NIS standardisation - Recommendations for improving NIS in EU standardisation policy,
Elérhető: https://www.enisa.europa.eu/publications/gaps-eu-standardisation/at_download/fullReport. [Hozzáférés dátuma: 2017.03.31.].

[58] **ENISA**, Communication network dependencies for ICS/SCADA Systems, Elérhető: https://www.enisa.europa.eu/publications/ics-scada-dependencies/at_download/fullReport. [Hozzáférés dátuma: 2017.03.31.].

[59] **Global Forum on Cyber Expertise** , The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers,
Elérhető:https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf. [Hozzáférés dátuma: 2017.03.31.].

[60] **1995. évi XXVIII. törvény** a nemzeti szabványosításról.

[61] **ISO/IEC 14764:2006** Software Engineering -- Software Life Cycle Processes – Maintenance.

[62] **ISO/IEC/IEEE 29119-1:2013** Software and systems engineering -- Software testing -- Part 1: Concepts and definitions.

[63] **ISO/IEC 33001:2015** Information technology -- Process assessment -- Concepts and terminology.

[64] **ISO/IEC 33002:2015** Information technology -- Process assessment -- Requirements for performing process assessment.

[65] **ISO/IEC 33003:2015** Information technology -- Process assessment -- Requirements for process measurement frameworks.

[66] **ISO/IEC 33004:2015** Information technology -- Process assessment -- Requirements for process reference, process assessment and maturity models.

[67] **ISO/IEC 33020:2015** Information technology -- Process assessment -- Process measurement framework for assessment of process capability.

[68] **IT4IT** - Managing the Business of IT. *(szabvány)*

[69] **ISACA Magyarországi Egyesület**, ISACA magyar szakkifejezés-gyűjtemény, ISACA Magyarországi Egyesület, 1027 Budapest, Horvát u. 14-24., 2013. ISBN: 978-963-08-6769-6

[70] **Holtai András; Magyar, Sándor; Puskás, Béla**, Az informatikai fejlesztés és üzemeltetés határvonalai, Felderítő Szemle, XV. évfolyam 1. szám, pp. 191-203, HU ISSN 1588-242X

[71] **Dr. Michelberger Pál - Lábodi Csaba**, Vállalati információbiztonság szervezése.
Elérhető: http://kgk.uni-obuda.hu/sites/default/files/10_Michelberger_Labodi.pdf, [Hozzáférés dátuma: 2017.03.31.].

[72] **MSZ ISO/IEC 20000-1:2013**, Informatika. Szolgáltatásirányítás. 1. rész: A szolgáltatásirányítási rendszer követelményei.

[73] **MSZ EN ISO/IEC 27000:2017** Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Áttekintés és szakszótár (ISO/IEC 27000:2016), 2017.

[74] **MSZ ISO/IEC 27001**:**2014** Informatika. Biztonságtechnika.Az információbiztonság irányítási rendszerei. Követelmények.

[75] **MSZ EN ISO/IEC 27002:2017** Informatika. Biztonságtechnika. Gyakorlati útmutató az információbiztonsági kontrollokhoz/intézkedésekhez (ISO/IEC 27002:2013, tartalmazza a 2014. évi 1. és a 2015. évi 2. helyesbítést).

[76] **ISO/IEC 27005:2008** Information technology -- Security techniques -- Information security risk management.

[77] **AJP-3.10** ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS, 2015.

[78] **Puskás Béla**, Információbiztonsági környezet kialakítása, HÍRVILLÁM = SIGNAL BADGE, 1. szám 6/2, pp. 108-133, 2015. HU ISSN 2061-9

[79] **AAP-31 Ed. 3** NATO Communication and Information Systems Glossary, 2016.

[80] **AC/35-D/2005-REV3** Management Directive on CIS Security, 2015.

[81] **JSP 480-16th Edition** Defence Co-Ordinatinginstallation Design Authority.

[82] **JSP 440 Edition 4.3** The Defence Manual of Security.

[83] **AJP-6 Ed. A,** Allied Joint Docrine for Communication and Information Systems, 2017.

[84] **Szádeczky Tamás**, „Információbiztonsági szabványok," Elérhető: http://vtki.uni-nke.hu/uploads/media_items/informaciobiztonsagi-tudatossag-gyakorlat.original.pdf. [Hozzáférés dátuma: 2017.03.31.].

[85] **Porkoláb Imre**, A hadviselés adaptációja: harc az emberi elméért, HADTUDOMÁNYI SZEMLE, 2014. VII. évfolyam 3. szám., pp. 56-69, HU ISSN 2060-0437

[86] **Symantec**, Internet Security Threat Report 2016 Elérhető: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. [Hozzáférés dátuma: 2017.03.31.].

[87] **AXELOS Limited**, Elérhető: ITIL® szakkifejezések és rövidítések magyarul. Elérhető: https://www.exin.com/assets/exin/frameworks/108/glossaries/hungarian_glossary_v1.0_201404.pdf [Hozzáférés dátuma: 2017.03.31.].

[88] **KFKI Számítástechnikai Rt**, Az ITIL módszertan áttekintése, Elérhető: http://www.itsmf.hu/documents/itil2modszertan_osszefoglalo_v3.1.pdf. [Hozzáférés dátuma: 2017.03.31.].

[89] **itSMF Hungary**, ITIL® Glossary of Terms, Definitions and Acronyms in Hungarian, V3.1.24.h 2.5, Budapest: itSMF Hungary, 2008., Elérhető: http://www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom/ITIL/ITIL%20V3%20fogalomt%C3%A1r%20v2.5.pdf. [Hozzáférés dátuma: 2017.03.31.].

[90] **Delta-3N Kft.**, Karbantartási stratégiák fejlődése Elérhető: http://www.delta3n.hu/gepvedelem/karbantartasi-strategiak-fejlod%C3%A9se. [Hozzáférés dátuma: 2017.03.31.].

[91] **ENISA**, Critical Information Infrastructures Protection approaches in EU ENISA 2015, Elérhető: https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf. [Hozzáférés dátuma: 2017.03.31.].

[92] **Chandrika Nath**, Cyber Security in the UK, Elérhető: http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf. [Hozzáférés dátuma: 2017.03.31.].

[93] **Mártonffy Attila**, IT Business Online, Elérhető: http://www.itbusiness.hu/Fooldal/hetilap/business/Az_informatika_es_a_koltsegek.html. [Hozzáférés dátuma: 2017.03.31.].

[94] **ACMP-5** NATO Requirements for Configuration Audits.

[95] **ISACA**, COBIT 5, United States of America, 2012. ISBN 978-1-60420-237-3

[96] **Puskás Béla; Rajnai Zoltán**, Requirements of the installation of the critical informational infrastructure and its management, Interdisciplinary description of complex systems, pp. 48-56, 2015/13., 48-56.pdf. ISSN 1334-4684, 2015.

[97] **Beinschroth József**, Kríziskezelés- Informatikai krízishelyzetek kezelése, Elérhető: http://uni-obuda.hu/users/beinschrothj/Kriziskezeles/Kriziskezeles_c.pdf. [Hozzáférés dátuma: 2017.03.31.].

[98] **MAVIR ZRt.,** P5 – 5. Eljárásrend: Vészhelyzeti üzem, Elérhető: http://mavir.hu/documents/10258/20774/policy5_final+version_H.pdf/8fe133d9-cda2-4581-9703-ff69226a41c2. [Hozzáférés dátuma: 2017.03.31.].

[99] **Puskás Béla; Rajnai Zoltán**, Decision-making support software application option for critical informational infrastructures, Acta Technica Corviniensis – Bbulletin of Engineering, pp. 89-94, 2015. ISSN 2067-3809

[100] **National Critical Information Infrastructure Protection Centre New Delhi**, Guidelines for the Protection of National Critical Information Infrastructure, Elérhető: https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf. [Hozzáférés dátuma: 2017.03.31.].

[101] **García Zaballos, Antonio; Jeun, Inkyung**, Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Caribbean and Selected Countries, Elérhető: https://publications.iadb.org/bitstream/handle/11319/7848/Best-Practices-for-Critical-Information-Infrastructure-Protection-%28CIIP%29-Experiences-from-Latin-America-and-the-Caribbean-and-Selected-Countries.pdf?sequence=1&isAllowed=y. [Hozzáférés dátuma: 2017.03.31.].

[102] **Steve Greenberg, Evan Mills, Bill Tschudi, Peter Rumsey, Bruce Myatt, Wei Bai, Wenli Geng**, Best Practices for Data Centers: Lessons Learned from Benchmarking 22 Data Centers, Elérhető: http://www.ing.unitn.it/~fontana/GreenInternet/Benchmarks/ACEEE-datacenters.pdf. [Hozzáférés dátuma: 2017.03.31.].

[103] **BS 7083:1996** Guide to the accommodation and operating environment for information technology (IT) equipment

[104] **AC/35-D/2001-REV2** Directive on Physical Security, 2008.

[105] **AC/322-D/0048-REV2** Technical Implementation Directive for Computer and Local Area Network (LAN) Security, 2011.

[106] **BS EN 50173-x:2007** Information technology Generic cabling systems.

[107] **90/2010. (III. 26.) Korm. rendelet** a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről.

[108] **Barabási Albert-László**, Villanások A jövő kiszámítható, Budapest: Nyitott Könyvműhely Kiadó KFT, 2010, p. 261. oldal., ISBN 978-963-310-014-1

[109] **Puskás Bél**a, Kockázatelemzés, kockázatértékelés: Informatikai üzemeltetés során fellépő kockázatok értékelése, Az 5. Báthory-Brassai Konferencia tanulmánykötetei., Budapest, Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2014, pp. 438-443., ISBN:978-615-5460-38-8

[110] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, „BSI-Standard 100-4: Business Continuity Management, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1. [Hozzáférés dátuma: 2017.03.31.]

[111] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, „BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile&v=1. [Hozzáférés dátuma: 2017.03.31.].

[112] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, „Risk analysis with the new threat catalogue T 0 "Elementary Threats, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile&v=1. [Hozzáférés dátuma: 2017.03.31.].

[113] **Abhinav Biswas, Sukanya Karunakaran**, Cybernetic modeling of Industrial Control Systems: Towards threat analysis of critical infrastructure, Elérhető: https://arxiv.org/ftp/arxiv/papers/1510/1510.01861.pdf. [Hozzáférés dátuma: 2017.03.31.].

[114] **Botos Zsolt**, Komputeralgebra Tanszék és a Magyar Tudományos Akadémia Számelméleti Kutatócsoport, Elérhető: http://compalg.inf.elte.hu/~attila/materials/ITbiztonsag_09_kockazat.pdf. [Hozzáférés dátuma: 2017.03.31.].

[115] **Pilar-tools,** Elérhető: http://www.pilar-tools.com/en/index.html. [Hozzáférés dátuma: 2017.03.31.].

[116] **ENISA**, EAR / PILAR, Elérhető: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_EAR_Pilar.html. [Hozzáférés dátuma: 2017.03.31.].

[117] **ENISA**, Threat and Risk ManagementRisk Management, Elérhető: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management. [Hozzáférés dátuma: 2017.03.31.].

[118] **Neumann János**, A számológép és az agy, Budapest: Gondolat Könyvkiadó, 1964., ISBN:0609001048471

[119] **Sunbird**, An Introduction to Data Center Infrastructure Management, Elérhető: https://www.sunbirddcim.com/sites/default/files/WP005_Revised_Sunbird_White Paper_Intro_toDCIM.pdf. [Hozzáférés dátuma: 2017.03.31.].

[120] **Schneider-electric**, Data Center Infrastructure Management (DCIM), Elérhető: http://www.schneider-electric.com/b2b/en/solutions/system/s4/data-center-and-network-systems-dcim/. [Hozzáférés dátuma: 2017.03.31.].

[121] **Neumann John von**, First Draft of a Report on the EDVAC,
Contract No. W-670-ORD-4926,
Between the United States Army Ordinance Department
and the University of Pennsylvania Moore School of Electrical Engineering
University of Pennsylvania
June 30, 1945

[122] **ACMP-4** NATO Requirements for Configuration Status Accounting and Configuration Data Management.

[123] **Jeff O'Brien**, 7 Tips for Managing Preventive Maintenance at Data Centers, Elérhető: http://www.datacenterknowledge.com/archives/2014/01/23/7-tips-managing-preventive-maintenance-data-centers/.
[Hozzáférés dátuma: 2017.03.31.].

[124] **Puskás Béla**, Integrált felügyeleti rendszer, Hadmérnök, XII. Évfolyam 1. szám, pp. 268-277, 2017. ISSN 1788-191

[125] **ACMP-3** NATO Requirements for Configuration Control - Engineering Changes, Deviations and Waivers.

[126] **ACMP-7** NATO Configuration Management - Guidance on the Application of ACMP-1 to 6.

[127] **Bognár Balázs**, Országos Katasztrófavédelemi Főigazgatóság, A kritikus infrastruktúra,
Elérhető: http://www.katasztrofavedelem.hu/index2.php?pageid=lrl_index.
[Hozzáférés dátuma: 2017.03.31.].

[128] **Device42**, Automated Data Center Management, Elérhető: http://www.device42.com/solutions/automated-data-center-management/?utm_source=Google&utm_medium=cpc&utm_campaign=Data_Center_Management_GA&utm_adgroup=Data_Center_Software&ad=140979572855&utm_term=data%20center%20management%20tools&matchtype=e&gclid=CJ3K. [Hozzáférés dátuma: 2017.03.31.].

[129] **Barabási Albert-László**, Elérhető: www.ceeol.com. [Hozzáférés dátuma: 2017.03.31.].

[130] **Cho Adrian**, „Mathematician claims breakthrough in complexity theory," Science, Elérhető: http://news.sciencemag.org/math/2015/11/mathematician-claims-breakthrough-complexity-theory. [Hozzáférés dátuma: 2017.03.31.]

[131] **ACMP-6** NATO Configuration Management Terms and Definitions.

[132] **Gartner**, Reviews for Data Center Infrastructure Management (DCIM) Software, Elérhető: https://www.gartner.com/reviews/market/data-center-infrastructure-management-tools. [Hozzáférés dátuma: 2017.03.31.].

[133] **Hewlett Packard Enterprise Development LP.**, HPE Operations Orchestration, Elérhető: https://www.hpe.com/h20195/V2/getpdf.aspx/4AA1-5782ENW.pdf. [Hozzáférés dátuma: 2017.03.31.].

[134] **1998. évi LXXXV. törvény** a Nemzeti Biztonsági Felügyeletről.

[135] **2003. évi C. törvény** az elektronikus hírközlésről.

[136] **179/2003. (XI. 5.) Korm. rendelet** a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól.

[137] **27/2004. (X. 6.) IHM rendelet** az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről.

[138] **100/2004. (IV. 27.) Korm. rendelet** az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról.

[139] **2073/2004. (IV. 15.) Korm. határozat** a Magyar Köztársaság nemzeti biztonsági stratégiájáról.

[140] **2007. évi LXXXVI. törvény** a villamos energiáról.

[141] **2010. évi CLVII. törvény** a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről.

[142] **92/2010. Korm. rendelet** az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól.

[143] **161/2010. Korm. rendelet** a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól.

[144] **346/2010. Korm. rendelet** a kormányzati célú hálózatokról.

[145] **1249/2010. (XI. 19.) Korm. határozat** az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végre.

[146] **309/2011. (XII. 23.) Korm. rendelet** a központosított informatikai és elektronikus hírközlési szolgáltatásokról.

[147] **360/2013. (X. 11.) Korm. rendelet** az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[148] **363/2013. (X. 11.) Korm. rendelet** a Külügyminisztérium diplomáciai célokra használt informatikai eszközeinek, hardver- és szoftver összetevőinek karbantartása, felügyelete, üzemeltetése, részleges rendszergazdai támogatása szolgáltatás ellátására.

[149] **484/2013. (XII. 17.) Korm. rendelet** a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről.

[150] **512/2013. (XII. 29.) Korm. rendelet** az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről.

[151] **541/2013. (XII. 30.) Korm. rendelet** a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről.

[152] **7/2013. (II. 26.) NFM rendelet** a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről.

[153] **41/2015. (VII. 15.) BM rendelet** az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre.

[154] **185/2015. (VII. 13.) Korm. rendelet** a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytat.

[155] **187/2015. (VII. 13.) Korm. rendelet** az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek.

[156] **246/2015. (IX. 8.) Korm. rendelet** az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[157] **330/2015. (XI. 10.) Korm. rendelet** a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[158] **359/2015. (XII. 2.) Korm. rendelet** a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről.

[159] **2016. évi XXX. törvény** a védelmi és biztonsági célú beszerzésekről.

[160] **38/2016. (XII. 29.) MvM rendelet** a fővárosi és megyei kormányhivatalok informatikai működésére vonatkozó szakmai követelményekről.

[161] **368/2016. (XI. 29.) Korm. rendelet** egyes, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló kormányrendeletek módosításáról.

[162] **1988. évi I. törvény** a közúti közlekedésről.

[163] **1995. évi XCVII. törvény** a légiközlekedésről.

[164] **2000. évi XLII. törvény** a víziközlekedésről.

[165] **2010. évi CLXXXV. törvény** a médiaszolgáltatásokról és a tömegkommunikációról.

[166] **2011. évi CXII. törvény** az információs önrendelkezési jogról és az információszabadságról.

[167] **118/2011. (VII. 11.) Korm. rendelet** a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről.

[168] **9/2011. (III. 9.) NGM rendelet** a váminformációs rendszerrel kapcsolatos részletszabályokról.

[169] **62/2011. (XII. 29.) BM rendelet** a katasztrófák elleni védekezés egyes szabályairól.

[170] **2012. évi CLIX. törvény** a postai szolgáltatásokról.

[171] **93/2012. (V. 10.) Korm. rendelet** az utak építésének, forgalomba helyezésének és megszüntetésének engedélyezéséről.

[172] **123/2014. (IV. 10.) Korm. rendelet** a közforgalmú személyszállítási szolgáltatásokhoz kapcsolódó adatok, adatbázisok és elektronikus adatkommunikációs technológiák egységességét és átjárhatóságát biztosító műszaki és technológiai előírásokról.

[173] **155/2014. (VI. 30.) Korm. rendelet** a radioaktív hulladékok átmeneti tárolását vagy végleges elhelyezését biztosító tároló létesítmények biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről.

[174] **27/2014. (IV. 18.) KIM rendelet** a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről.

[175] **2015. évi CCXXII. törvény** az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól, 2015**.**

[176] **46/2015.(XII. 30.) NGM rendelet** a Nemzeti Adó- és Vámhivatal bűnmegelőzési, bűnüldözési, valamint szabálysértési tevékenységével összefüggésben keletkezett adatok kezelésére jogosult szervek meghatározásáról és az adatok kezelésének technikai szabályairól.

[177] **2001/264/EK** Az Európai Unió Tanácsának a Tanács biztonsági szabályzatának elfogadásáról szóló tanácsi határozat.

[178] **Az Európai Parlament és a Tanács 460/2004/EK rendelete** az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról.

[179] **A Tanács 2005/222/IB kerethatározata** (2005. február 24.) az információs rendszerek elleni támadásokról.

[180] **COM (2005) 576 végleges. ZÖLD KÖNYV.** A létfontosságú infrastruktúrák védelmére vonatkozó. Európai programról.

[181] **2008/114/EK tanácsi irányelv** az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről.

[182] **COM (2009) 149 a Bizottság közleménye** az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a régiók bizottságának a kritikus informatikai infrastruktúrák védelméről.

[183] **IP/10/581 Digitális Menetrend:** A Bizottság akcióterve az európai jólét fellendítésére.

[184] **COM (2010) 517 az Európai Parlament és a Tanács irányelve** az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat hatályon kívül helyezéséről.

[185] **COM (2010) 521 az Európai Parlament és a Tanács rendelete** az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA).

[186] **COM (2010) 673 Bizottság közleménye** az Európai Parlamentnek és a Tanácsnak az EU belső biztonsági stratégiájának megvalósítása: öt lépés a biztonságosabb Európa felé.

[187] **2012/2096(INI) Kiberbiztonság és -védelem** Az Európai Parlament 2012. november 22-i állásfoglalása a kiberbiztonságról és -védelemről.

[188] **JOIN/2013/01 közös közlemény** az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a régiók bizottságának az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.

[189] **EU**, Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér című közlemény, 2013.

[190] **C-M(2002) 49** Security Within The North Atlantic Treaty Organisation.

[191] **SDIP-27** NATO TEMPEST requirements and Evaluation procedures.

[192] **SDIP-28** NATO Zoning Procedures.

[193] **SDIP-29** Facility Design Criteria and Installation of Electrical Equipment for Processing Classified Information.

[194] **SDIP-30** Installation of Electronic Equipment for Processing of Classified Data.

[195] **AAP-06** NATO Glossary of terms and definitions (English and French), 2016.

[196] **AC/322-D 0052** NATO Communication and Information Systems Configuration Management Policy, 2006.

[197] **STANAG 4159** NATO Materiel Configuration Management Policy and Procedures for Multinational Joint Projects.

[198] **ACMP-1** NATO Requirements for the Preparation of Configuration Management Plans.

[199] **ACMP-2** NATO Requirements for Configuration Identification.

[200] **AC/35-D/2004-REV3 Primary Directive on CIS Security, 2013.**

[201] **ACO Directive 080-095** Communication and Information System (CIS) Planning Directive, 2014.

[202] **AAITP-06** System Architecture Requirements for Asset, Consignment and Personnel Tracking Information Excchange, 2014.

[203] **JSP480 Edition_16** Manual of Regulations for Installation of Communication & Information Systems.

[204] **BS 6701**:2010 Telecommunications equipment and telecommunications cabling-specification for installation, operation and maintenance.

[205] **BS EN 50174-x**:2009/2003 Information technology Cabling installation.

[206] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, BSI Standard 100-1 Information Security Management Systems (ISMS), Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1. [Hozzáférés dátuma: 2017.03.31.].

[207] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, „BSI-Standard 100-2: IT-Grundschutz Methodology," Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile&v=1 [Hozzáférés dátuma: 2017.03.31.].

[208] **Federal Office for Information Security (BSI)**, „Secure Connection of Local Networks to the Internet v1.0 (ISi-Check), Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/InternetSecurity/ISi-LANA-ISi-Check.pdf?__blob=publicationFile&v=1. [Hozzáférés dátuma: 2017.03.31.]

[209] **Pilar-tools**, Risk Analysis and Management Additional Tools Help Files, Elérhető: http://www.pilar-tools.com/doc/rmat/v55/help_en_e_2017-01-02.pdf. [Hozzáférés dátuma: 2017.03.31.].

[210] **Hendershott Consulting Inc**, Overview of the ITIL v3 Library, Elérhető: http://www.hci-itil.com/ITIL_v3/images/service_improvement_ch7_fig_7_1.jpg. [Hozzáférés dátuma: 2017.03.31.].

[214] **Szegedi Egyetem,** Kombinatorika elemei / Kombinatorika előadás, 2015/2016 ősz, Elérhető: http://www.math.u-szeged.hu/~ngaba/kombi_ea_old/index.html. [Hozzáférés dátuma: 2017.03.31.].

[223] **MuxViz**, Elérhető: http://muxviz.net/index.php. [Hozzáférés dátuma: 2017.03.31.].

IRODALOMJEGYZÉK

[211] **IT Governance Institute**, Office of Government Commerce, isaca.org, Elérhető: http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf. [Hozzáférés dátuma: 2017.03.31.].

[212] **Magyar Szabványügyi Testület**, Elérhető: http://www.mszt.hu/web/guest/msz-iso-iec-20000-1. [Hozzáférés dátuma: 2017.03.31.].

[213] **Galambos Gábor, Árgilán Viktor**, Matematika I., Elérhető: http://www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0013_galambos_matematika_i/1010_hamilton_krutak.html. [Hozzáférés dátuma: 2017.03.31.].

[215] **Obádovics J. Gyula**, Valószínűségszámítás és Matematikai Statisztika, Budapest: SCOLAR KFT., 2009., ISBN: 978-963-244-067-5

[216] **Informatikai Tárcaközi Bizottság (ITB) 5. számú ajánlása** – Bevezetés a PRINCE projektirányítási módszertanba., Elérhető: http://www.ekk.gov.hu/hu/kib/archivum. [Hozzáférés dátuma: 2017.03.31.].

[217] **Symantec**, Internet Security Threat Report 2013, Elérhető: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf. [Hozzáférés dátuma: 2017.03.31.].

[218] **Karinthy Ferenc**, Láncszemek, Elérhető: http://mek.oszk.hu/07300/07367/html/01.htm#54. [Hozzáférés dátuma: 2017.03.31.].

[219] **Kaspersky**, Corporate threats, 2014., Elérhető: http://report.Kaspersky.com/#corporate-threats. [Hozzáférés dátuma: 2017.03.31.].

[220] **Crysys Lab**, miniduke, Elérhető: http://www.crysys.hu/miniduke/miniduke_indicators_public.pdf. [Hozzáférés dátuma: 2017.03.31.].

[221] **Mcafee**, Threats predictions, Elérhető: https://www.mcafee.com/ru/resources/reports/rp-threats-predictions-2016.pdf. [Hozzáférés dátuma: 2017.03.31.].

[222] **Milgram Stanley**, The Small World Problem, Psychology Today, New York, 1967. Elérhető: http://snap.stanford.edu/class/cs224w-readings/milgram67smallworld.pdf. [Hozzáférés dátuma: 2017.03.31.].

[224] **Pokorádi László**, Üzemeltetési folyamat gráfmodellezése, Elérhető: http://www.repulestudomany.hu/kulonszamok/2014_cikkek/2014-2-19-0114_Pokoradi_Laszlo.pdf. [Hozzáférés dátuma: 2017.03.31.].

[225] **Public Safety Canada**, Forging a Common Understanding for Critical Infrastructure, Elérhető: https://www.dhs.gov/sites/default/files/publications/critical-five-shared-. [Hozzáférés dátuma: 2017.03.31.].

[226] **Information Security Policy Council**, The Basic Policy of Critical Information Infrastructure Protection, Elérhető: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf. [Hozzáférés dátuma: 2017.03.31.].

[227] **The National Cyber Security Centre**, Elérhető: https://www.ncsc.gov.uk/. [Hozzáférés dátuma: 2017.03.31.].

[228] **U.S. Department of Homeland**, Recommended Practice for Securing Control System Modems, Elérhető: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_SecuringModems_S508C.pdf. [Hozzáférés dátuma: 2017.03.31.].

[229] **Deborah Housen-Courie - ATO Cooperative Cyber Defence Centre of Excellence**, National Cyber Security Organisation in the Israel, Elérhető: https://ccdcoe.org/sites/default/files/multimedia/pdf/IL_NCSO_final.pdf . [Hozzáférés dátuma: 2017.03.31.].

[230] **Mikk Raud - ATO Cooperative Cyber Defence Centre of Excellence**, China and Cyber: Attitudes, Strategies, Organisation, Elérhető: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf. [Hozzáférés dátuma: 2017.03.31.].

[231] **Bob Woolley**, Top 10 Mistakes in Data Center Operations: Operating Efficient and Effective Data Centers, Elérhető: http://www.apc.com/salestools/VAVR-8RNGFT/VAVR-8RNGFT_R0_EN.pdf. [Hozzáférés dátuma: 2017.03.31.].

[232] **Nlyte**, The Nlyte Solution Suite, Elérhető: http://www.nlyte.com/. [Hozzáférés dátuma: 2017.03.31.].

[233] **Katharina Ziolkowski** - NATO CCD COE Publication, Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, Elérhető: https://ccdcoe.org/publications/books/Peacetime-Regime.pdf. [Hozzáférés dátuma: 2017.03.31.].

[234] **Fejér Tamás**, ORGANIGRAM készítés felsőfokon, Szervezettervezés org.manager szoftverrel, Elérhető: http://www.perbithr.hu/share/HPSZ_10.02.ORG.pdf. [Hozzáférés dátuma: 2017.03.31.].

[235] **Eric Luiijf, Bert Jan te Paske**, Cyber Security of Industrial Control Systems, Elérhető: http://publications.tno.nl/publication/34616507/KkrxeU/%20luiijf-2015-cyber.pdf. [Hozzáférés dátuma: 2017.03.31.].

[236] **Laurent Lessard**, Optimal Control of Two-Player Systems With Output Feedback, IEEE TRANSACTIONS ON AUTOMATIC CONTROL, 60, pp. 2129-2144, 2015.

[237] **Information Security Policy Council- Government of JAPAN**, The Basic Policy of Critical Information Infrastructure Protection (3rd Edition), Elérhető: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3_r1.pdf. [Hozzáférés dátuma: 2017.03.31.]

[238] **Ian Ellefsen, Sebastiaan Solms**, Implementing Critical Information Infrastructure Protection Structures in Developing Countries, Elérhető: https://hal.inria.fr/hal-01483817/document. [Hozzáférés dátuma: 2017.03.31.].

[239] **Federal Office for Information Security (BSI)**, Open Platform Communications Unified Architecture Security AnalysisOpen Platform Communications Unified Architecture Security Analysis, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/OPCUA/OPCUA.pdf?__blob=publicationFile&v=2. [Hozzáférés dátuma: 2017.03.31.].

[240] **Federal Office for Information Security (BSI)**, The State of IT Security in Germany 2016, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2016.pdf?__blob=publicationFile&v=3. [Hozzáférés dátuma: 2017.03.31.].

[241] **Federal Office for Information Security (BSI)**, Cloud Computing Compliance Controls Catalogue, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/ComplianceControlsCatalogue.pdf?__blob=publicationFile&v=4. [Hozzáférés dátuma: 2017.03.31.].

[242] **Federal Office for Information Security (BSI)**, ICS Security Compendium, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.pdf?__blob=publicationFile&v=3. [Hozzáférés dátuma: 2017.03.31.].

[243] **Sistema di informazione per la sicurezza della Repubblica**, 7 Law No. 124/2007, Elérhető: http://www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html#_ftn10. [Hozzáférés dátuma: 2017.03.31.].

[244] **BBC, „BBC NEWS technology**, Elérhető: http://www.bbc.co.uk/news/technology-15844230. [Hozzáférés dátuma: 2017.03.31.].

[245] **Budafok-Tétény Polgármesteri Hivatal**, Folyamatelemzést és modellezést támogató szoftveralkalmazási javaslat, Elérhető: http://www.etudasportal.gov.hu/download/attachments/17039444/19.+Folyamatelemz%C3%A9st+%C3%A9s+modellez%C3%A9st+t%C3%A1mogat%C3%B3+szoftverjavaslat.pdf. [Hozzáférés dátuma: 2017.03.31.].

[246] **Balogh Sándor**, Logikai elemek és kapcsolások \ gráfelméleti alapfogalmak, Beregszász: Kárpátaljai Magyar Pedagógusszövetség Tankönyv- és Taneszköztanácsa, 2004. Elérhető: http://mek.oszk.hu/02900/02901/02901.pdf. [Hozzáférés dátuma: 2017.03.31.].

[247] **Presidency of the Council of Ministers**, National strategic framework for cyberspace security, Elérhető: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf. [Hozzáférés dátuma: 2017.03.31.].

[248] **Presidency of the Council of Ministers**, The national plan for cyberspace protection and ict security, Elérhető: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf. [Hozzáférés dátuma: 2017.03.31.].

RÖVIDÍTÉSEK ÉS FOGALMAK JEGYZÉKE

Rövidítés/Fogalom	Angol	Magyar
ANSI	American National Standards Institute	Amerikai Szabványügyi Hivatal
ARPA	Advanced Research Projects Agency	Fejlett Kutatási Projektek Ügynöksége
BASELINE		Az értekezésben használt változata egy konfiguráció alapállapotát jelenti, egy pillanatfelvétel, amely hivatkozási alapként szolgál
BBC	British Broadcasting Corporation	Brit közszolgálati műsorszolgáltató
BCM	Business Continuity Plan	Üzletmenet-folytonossági terv
BM		Belügyminisztérium
CIA	Confidentiality Integrity Availability	Bizalmasság Sértetlenség Rendelkezésre állás
CBM	Condition Based Maintenance	Állapotfüggő karbantartás
CC	Common Criteria	Nemzetközileg elfogadott keretrendszer az IT biztonság területén
CEN	Comité Européen de Normalisation	Európai Szabványügyi Bizottság
CENELEC	Comité Européen de Normalisation Electrotechnique	Európai Elektrotechnikai Szabványügyi Bizottság
CERT	Computer Emergency Response Team	Amerikai használatban Számítógépes Eseménykezelő Központ
CIO	Chief Information Officer	Informatikai felső vezető
CISA	Certified Information Systems Auditor	Információs rendszerbiztonsági auditor program
CISM	Certified Information Security Manager	Informatikai biztonsággal foglalkozó szakemberek minősítő programja

Rövidítés/Fogalom	Angol	Magyar
CITM	Certified IT Manager	Informatikai rendszerek üzemeltetésével foglalkozó szakemberek részére kidolgozott program
CIWIN	Critical Infrastructure Warning Information Network	Létfontosságú infrastruktúrák figyelmeztető információs hálózat
CMDB	Configuration Management DataBase	Konfiguráció Management Adatbázis
CMS	Configuration Management System	Konfigurációt Kezelő Rendszer
COBIT	Control Objectives for Information and Related Technology	Vállalati információtechnológia irányításának és menedzsmentjének átfogó üzleti és vezetési keretrendszere.
CSIRT	Computer Security Incident Response Team	Európai használatban Számítógépes Eseménykezelő Központ
DCA Certification Guidelines for Data Centres	Data Centre Alliance Certification Guidelines for Data Centres	Adatközpontokkal hitelesítési eljárások
DCIM	Data Center Infrastructure Management	Adatközpont infrastruktúrakezelő
DDoS	Distributed Denial of Service	Elosztott Szolgáltatásmegtagadás
EK		Európai Közösség
EMC	ElectroMagnetic Compatibility	Elektromágneses összeférhetőség
ENISA	European Union Agency for Network and Information Security	Európai Hálózat- és Információbiztonsági Ügynökség
ETSI	European Telecommunications Standards Institute	Európai Távközlési Szabványügyi Intézet
EURATOM	European Atomic Energy Community	Európai Atomenergia Közösség
FBCM	Failure Based Corrective Maintenance	Hibaelhárító karbantartás

Rövidítés/Fogalom	Angol	Magyar
Georedundancia		Földrajzi értelemben jól elkülönült párhuzamosan meglévő egységek.
GovCERT-Hungary		Kormányzati Eseménykezelő Központot
Hop		Ugrás, Routerek esetén hány routeren keresztül érhető el a másik
HUMINT	Human Intelligence	Emberek kapcsolat által végrehajtott hírszerzés
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Bizottság
IEEE	Institute of Electrical and Electronics Engineers	Villamosmérnökök és Informatikusok Nemzetközi Szervezete
IGP	Interior Gateway Protocol	Autonóm rendszereken belüli adatcsomag továbbításra szolgáló protokoll.
IHM		Informatikai és Hírközlési *Minisztérium*
IKT		Információs és Kommunikációs Technológia
Interdependencia		Egymástól való függőség
ISACA	Information Systems Audit and Control Association	Információs rendszerek (technológiák) auditálásával kontrollálásával foglalkozó társaság
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
ISZT		Internet Szolgáltatók Tanácsának
IT	Information Technology	Információ-Technológia Technológia használata információ tárolására, átvitelére vagy feldolgozására. Ebbe a technológiába jellemzően számítógépek, távközlési rendszerek, alkalmazások és egyéb szoftvereket tartoznak. [87]

Rövidítés/Fogalom	Angol	Magyar
IT4IT		2014-ben bevezetett szabvány az IT-t egy egységként kezelő modellje
ITB		Informatikai Tárcaközi Bizottság
ITIL	Information Technology Infrastructure Library	Informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló módszertan, legjobb gyakorlat.
ITU	International Telecommunication Union	Nemzetközi Távközlési Unió
Kiszolgáló		Számítógépes hálózatokban pl. a szerverek
Kliens		Számítógépes hálózatban lévő végfelhasználó eszköz
Königsberg		Kalinyingrád a balti tengeri kikötőváros, ma az orosz exklávéhoz tartozik
KRESZ		Közúti Rendelkezések Egységes Szabályozása
LEED	Leadership in Energy and Environmental Design	Energia és környezetvédelmi ajánlás
LRLIBEK		Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ
Mavtv.		Minősített adat védelméről szóló 2009. évi CLV. törvényt
MIL-CERT		Katonai Számítógépes Eseménykezelő Központ
Minősített anyag		Olyan adat, amelyet a minősített adat védelméről szóló 2009. évi CLV törvény 3. § határoz meg
MSZT		Magyar Szabványügyi Testület
NATO	North Atlantic Treaty Organization	Észak-atlanti Szerződés Szervezete
NATO HQ	NATO Headquarters	Észak-atlanti Szerződés Szervezete főhadiszállása (központja)
NBF		Nemzeti Biztonsági Felügyelet

Rövidítés/Fogalom	Angol	Magyar
NFM		Nemzeti Fejlesztési Minisztérium
NIC	Network Interface Card	Hálózati kártya
NYEU		Nyugat-európai Unió
PCBM	Parameter Condition Based Maintenance	Paraméter kondíció szerinti karbantartás
PDCA	Plan-Do-Check-Act	Tervezés Végrehajtás Ellenőrzés Beavatkozás
PILAR		Kockázatelemző alkalmazás neve
PM	Preventive / Planned Maintenance	Megelőző karbantartás
PSYOPS	Psychological operations	Lélektani műveletek
RCM	Reliability Centered Maintenance	Megbízhatóság központú karbantartás
RIP	Routing Information Protocol	útvonal választási információk cseréjére szolgáló protokoll
Router	Router	Forgalomirányító eszköz
SDIP - SECAN	SECAN Doctrine and Information Publication	Biztonsági szabványgyűjtemény
SECAN	SECurity and Evaluation Agency (Military Committee Communications Security & Evaluation Agency)	Biztonsági és értékelő ügynökség
Site		Fizikailag (helyileg) elkülönült rendszerelem.
SKMS	Service Knowledge Management System	(Szolgáltatás) Tudásmenedzsment Rendszer
TCO	Total cost of ownership	Összköltsége
TEMPEST	TEMPorary Emanation and Spurious Transmission	Eredetileg kódszó, az elektronikai eszközök kisugárzásának elemzésére.
TIA	Telecommunications Industry Association	Telekommunikációs Ipari Szövetség

Rövidítés/Fogalom	Angol	Magyar
TIER I, II, III, IV		Első, másodig, harmadik, negyedik szint. Az Amerikai Telekommunikációs Ipari Szövetség által kiadott adatközpontra vonatkozó szabványban leírt szintek.
TPM	Total Productive Maintenance	Teljes körű hatékony karbantartás
UPS	Uninterruptible Power Supply	Szünetmentes tápegység
VESDA	Very Early Smoke Detection Apparatus	Korai füstérzékelő berendezés

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

MELLÉKLETEK

1. SZÁMÚ MELLÉKLET HAZAI JOGSZABÁLYOK

- 1995. évi XXVIII. törvény a nemzeti szabványosításról; [60]
- 1998. évi LXXXV. törvény a Nemzeti Biztonsági Felügyeletről. Hatályon kívül helyezett; [134]
- 2003. évi C. törvény az elektronikus hírközlésről; [135]
- 179/2003. (XI. 5.) Korm. rendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól. Hatályon kívül helyezett; [136]
- 27/2004. (X. 6.) IHM rendelet az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről. Hatályon kívül helyezett; [137]
- 100/2004. (IV. 27.) Korm. rendelet az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról; [138]
- 2073/2004. (IV. 15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról. Hatályon kívül helyezett; [139]
- 2007. évi LXXXVI. törvény a villamos energiáról; [140]
- 2080/2008. (VI. 30.) Korm. határozathoz tartozó Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról; [21]
- 2009. évi CLV. törvény a minősített adat védelméről; [19]
- 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről; [141]
- 90/2010. Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről; [107]
- 92/2010. Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól; [142]

- 161/2010. Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól; [143]
- 346/2010. Korm. rendelet a kormányzati célú hálózatokról; [144]
- 1249/2010. (XI. 19.) Korm. határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról; [145]
- 309/2011. (XII. 23.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokról; [146]
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről; [22]
- 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról; [24]
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról; [18]
- 360/2013. (X. 11.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről; [147]
- 363/2013. (X. 11.) Korm. rendelet a Külügyminisztérium diplomáciai célokra használt informatikai eszközeinek, hardver- és szoftver összetevőinek karbantartása, felügyelete, üzemeltetése, részleges rendszergazdai támogatása szolgáltatás ellátására vonatkozó pályázathoz kapcsolódó informatikai beszerzéseknek a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 218/2011. (X. 19.) Korm. rendelet 7. § (5) bekezdés a) pontja szerinti minősítéséről; [148]
- 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a

kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről; [149]

- 512/2013. (XII. 29.) Korm. rendelet az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról; [150]
- 541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről; [151]
- 7/2013. (II. 26.) NFM rendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről; [152]
- A honvédelmi miniszter 39/2014. (V. 30.) HM utasítása a Magyar Honvédség Informatikai Szabályzatának kiadásáról; [12]
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről; [153]
- 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól; [154]
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról; [155]

- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről; [156]
- 330/2015. (XI. 10.) Korm. rendelet a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről; [157]
- 359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről; [158]
- 2016. évi XXX. törvény a védelmi és biztonsági célú beszerzésekről; [159]
- 38/2016. (XII. 29.) MvM rendelet a fővárosi és megyei kormányhivatalok informatikai működésére vonatkozó szakmai követelményekről; [160]
- 368/2016. (XI. 29.) Korm. rendelet egyes, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló kormányrendeletek módosításáról. Hatályon kívül helyezett. [161]

Továbbá a Kritikus Információs Infrastruktúrához szorosan nemköthető, de kapcsolódó jogszabályok:

- 1988. évi I. törvény a közúti közlekedésről; [162]
- 1995. évi XCVII. törvény a légiközlekedésről; [163]
- 2000. évi XLII. törvény a víziközlekedésről; [164]
- 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről; [141]
- 2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról; [165]
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról; [166]
- 118/2011. (VII. 11.) Korm. rendelet a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről; [167]
- 9/2011. (III. 9.) NGM rendelet a váminformációs rendszerrel kapcsolatos részletszabályokról; [168]

- 62/2011. (XII. 29.) BM rendelet a katasztrófák elleni védekezés egyes szabályairól; [169]
- 2012. évi CLIX. törvény a postai szolgáltatásokról; [170]
- 93/2012. (V. 10.) Korm. rendelet az utak építésének, forgalomba helyezésének és megszüntetésének engedélyezéséről; [171]
- 123/2014. (IV. 10.) Korm. rendelet a közforgalmú személyszállítási szolgáltatásokhoz kapcsolódó adatok, adatbázisok és elektronikus adatkommunikációs technológiák egységességét és átjárhatóságát biztosító műszaki és technológiai előírásokról, a központi adatbázisokról és az azokhoz kapcsolódó központi szolgáltatásokról, továbbá a működtető szervezetek kijelöléséről; [172]
- 155/2014. (VI. 30.) Korm. rendelet a radioaktív hulladékok átmeneti tárolását vagy végleges elhelyezését biztosító tároló létesítmények biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről; [173]
- 27/2014. (IV. 18.) KIM rendelet a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről; [174]
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól; [175]
- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről; [156]
- 46/2015. (XII. 30.) NGM rendelet a Nemzeti Adó- és Vámhivatal bűnmegelőzési, bűnüldözési, valamint szabálysértési tevékenységével összefüggésben keletkezett adatok kezelésére jogosult szervek meghatározásáról és az adatok kezelésének technikai szabályairól. [176]

2. SZÁMÚ MELLÉKLET NEMZETKÖZI SZABÁLYZÓK

EU szabályzók

- 2001/264/EK Az Európai Unió Tanácsának a Tanács biztonsági szabályzatának elfogadásáról szóló tanácsi határozat; [177]
- Az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról; [178]
- A Tanács 2005/222/IB kerethatározata (2005. február 24.) az információs rendszerek elleni támadásokról; [179]
- COM (2005) 576 végleges. ZÖLD KÖNYV. A létfontosságú infrastruktúrák védelmére vonatkozó. Európai programról; [180]
- 2008/114/EK tanácsi irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről; [181]
- COM (2009) 149 a Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a régiók bizottságának a kritikus informatikai infrastruktúrák védelméről „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”; [182]
- IP/10/581 Digitális Menetrend: A Bizottság akcióterve az európai jólét fellendítésére; [183]
- COM (2010) 517 az Európai Parlament és a Tanács irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat hatályon kívül helyezéséről; [184]
- COM (2010) 521 az Európai Parlament és a Tanács rendelete az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA); [185]
- COM (2010) 673 Bizottság közleménye az Európai Parlamentnek és a Tanácsnak az EU belső biztonsági stratégiájának megvalósítása: öt lépés a biztonságosabb Európa felé; [186]
- 2012/2096(INI) Kiberbiztonság és -védelem Az Európai Parlament 2012. november 22-i állásfoglalása a kiberbiztonságról és -védelemről; [187]

- JOIN/2013/01 közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a régiók bizottságának az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér; [188]
- 2013. február 7. „Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér” című közlemény; [189]
- 2016/1148 Irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésről (NIS irányelv) [55]

NATO szabályzók

- C-M(2002) 49 Security Within The North Atlantic Treaty Organisation; [190]
- SDIP-27 NATO TEMPEST requirements and Evaluation procedures; [191]
- SDIP-28 NATO Zoning Procedures; [192]
- SDIP-29 Facility Design Criteria and Installation of Electrical Equipment for Processing Classified Information; [193]
- SDIP-30 Installation of Electronic Equipment for Processing of Classified Data; [194]
- AAP-06 NATO Glossary of Terms and Definitions (English and French); [195]
- AJP-3.10 Allied Joint Doctrine for Information Operations; [77]
- AC/322-D 0052 NATO Communication and Information Systems Configuration Management Policy; [196]
- STANAG 4159 NATO Materiel Configuration Management Policy and Procedures for Multinational Joint Projects; [197]
- ACMP-1 NATO Requirements for the Preparation of Configuration Management Plans; [198]
- ACMP-2 NATO Requirements for Configuration Identification; [199]
- ACMP-3 NATO Requirements for Configuration Control - Engineering Changes, Deviations and Waivers; [125]

- ACMP-4 NATO Requirements for Configuration Status Accounting and Configuration Data Management; [122]
- ACMP-5 NATO Requirements for Configuration Audits; [94]
- ACMP-6 NATO Configuration Management Terms and Definitions; [131]
- ACMP-7 NATO Configuration Management - Guidance on the Application of ACMP-1 to 6; [126]
- AC/35-D/2004-REV3 Primary Directive on CIS Security; [200]
- AC/35-D/2001-REV2 Directive on Physical Security; [104]
- AC/35-D/2005-REV3 Management Directive on CIS Security; [80]
- AC/322-D/0048-REV2 Technical Implementation Directive for Computer and Local Area Network (LAN) Security; [105]
- AAP-31 Ed. 3 NATO Communication and Information Systems Glossary; [79]
- AJP-6 Ed. A, Allied Joint Doctrine for Communication and Information Systems; [83]
- ACO Directive 080-095 Communication and Information System (CIS) Planning Directive; [201]
- AAITP-06 System Architecture Requirements for Asset, Consignment and Personnel Tracking Information Exchange. [202]

Brit katonai szabványok

- JSP 480-16th Edition Defence Co-Ordinating Installation Design Authority; [81]
- Manual of Regulations for Installation of Communication & Information Systems; [203]
- JSP 440 Edition 4.3 The Defence Manual of Security. [82]

Brit katonai szabványok

- BS 6701:2010 Telecommunications equipment and telecommunications cabling-specification for installation, operation and maintenance; [204]
- BS 7083:1996 Guide to the accommodation and operating environment for Information Technology (IT) equipment; [103]

- BS EN 50173-x:2007 Information technology Generic cabling systems; [106]
- BS EN 50174-x:2009/2003 Information technology Cabling installation. [205]

Német szabványok

- BSI [142] Standard 100-1 Information Security Management Systems (ISMS) [206]
- BSI-Standard 100-2: IT-Grundschutz Methodology [207]
- BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz [111]
- BSI-Standard 100-4: Business Continuity Management [110]
- BSI German Threats Catalogue – Elementary Threats [112]
- (BSI) „Secure Connection of Local Networks to the Internet v1.0 (ISi-Check) [208]

[142] BSI (Bundesamt für Sicherheit in der Informationstechnik)

3. SZÁMÚ MELLÉKLET HATÁLYOSSÁG ÖSSZEHASONLÍTÁSA

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról	**2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről**	**AZ EU 2016/1148 IRÁNYELVE a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről**	**2009. évi CLV. törvény a minősített adat védelméről**
(1) *a)* a központi államigazgatási szervek, a Kormány és a kormánybizottságok kivételével, *b)* a **Köztársasági Elnöki Hivatal**, *c)* az **Országgyűlés Hivatala**, *d)* az **Alkotmánybíróság Hivatal**, *e)* az **Országos Bírósági Hivatal és a bíróságok**, *f)* az **ügyészségek**, *g)* az **Alapvető Jogok Biztosának Hivatala**, *h)* az **Állami Számvevőszék**, *i)* a **Magyar Nemzeti Bank**, *j)* a **fővárosi és megyei kormányhivatalok**, *k)* a helyi és a nemzetiségi **önkormányzatok képviselő-testületének hivatala**, a hatósági igazgatási társulásokra, *l)* a **Magyar Honvédség**. (2) E törvény rendelkezéseit kell	**<u>Ágazatok</u>**: • **Energia** (villamosenergia-rendszer létesítményei, kőolajipar, földgázipar) • **Közlekedés** (közúti, vasúti, légi, vízi, logisztikai központok) • **Agrárgazdaság** (mezőgazdaság, élelmiszeripar, elosztó hálózatok) • **Egészségügy** (aktív fekvőbeteg-ellátás, mentésirányítás, egészségügyi tartalékok és vérkészletek, magas biztonsági szintű biológiai laboratóriumok, egészségbiztosítás informatikai rendszere, gyógyszer-nagykereskedelem) • **Pénzügy** (pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei; bank- és hitelintézeti biztonság; készpénzellátás) • **Infokommunikációs technológiák** (internet-infrastruktúra és internet hozzáférés szolgáltatás; vezetékes és vezeték nélküli elektronikus	**<u>Ágazatok:</u>** • **Energia** (villamosenergia-rendszer létesítményei, kőolajipar, földgázipar) • **Közlekedést** (közúti közlekedés, vasúti közlekedés, légi közlekedés, vízi közlekedés) • **Banki szolgáltatás** • **Egészségügy** • **Pénzügyi piaci infrastruktúra** • **Ivóvízellátás és -elosztás** • **Digitális infrastruktúrákat.** • **Online piactér** • **Online keresőprogram** • **Felhőlapú számítástechnikai szolgáltatások**	*minősítő:* feladat- és hatáskörében **minősítésre jogosult személy** *Minősített adatot kezelő szerv:* állami vagy közfeladat ellátása **érdekében minősített adat kezelését végző szerv, szervezet vagy szervezeti egység, továbbá a gazdálkodó szervezet**; *Felhasználó:* **az a személy**, **akinek** állami vagy közfeladat végrehajtása céljából a felhasználói engedély kiadására jogosult vezető **a minősített adatra vonatkozóan a felhasználói engedélyben rendelkezési jogosultságokat biztosít**; *Közreműködő:* az a természetes **személy**, **aki** az állami vagy közfeladatot ellátó szerv feladat- és **hatáskörébe**

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról	**2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről**	**AZ EU 2016/1148 IRÁNYELVE a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről**	**2009. évi CLV. törvény a minősített adat védelméről**
alkalmazni: *a)* az (1) bekezdésben meghatározott szervek és **ezen szervek számára adatkezelést végzők**, *b)* a jogszabályban meghatározott, **a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói**, *c)* az európai vagy nemzeti **létfontosságú rendszerelemmé a létfontosságú rendszerek** és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt rendszerelemek **elektronikus információs rendszereinek** védelmére.	hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok; rádiós távközlés; űrtávközlés; műsorszórás; postai szolgáltatások; kormányzati informatikai, elektronikus hálózatok) • **Víz** (ivóvíz-szolgáltatás; felszíni és felszín alatti vizek minőségének ellenőrzése; szennyvízelvezetés és -tisztítás; vízbázisok védelme; árvízi védművek, gátak) • **Jogrend – Kormányzat** (kormányzati rendszerek, létesítmények, eszközök; közigazgatási szolgáltatások; igazságszolgáltatás) • **Közbiztonság – Védelem** (rendvédelmi szervek infrastruktúrái) • **Honvédelem** (honvédelmi rendszerek és létesítmények)		**tartozó ügyben segítséget nyújt**, és ehhez minősített adat felhasználása is szükséges;

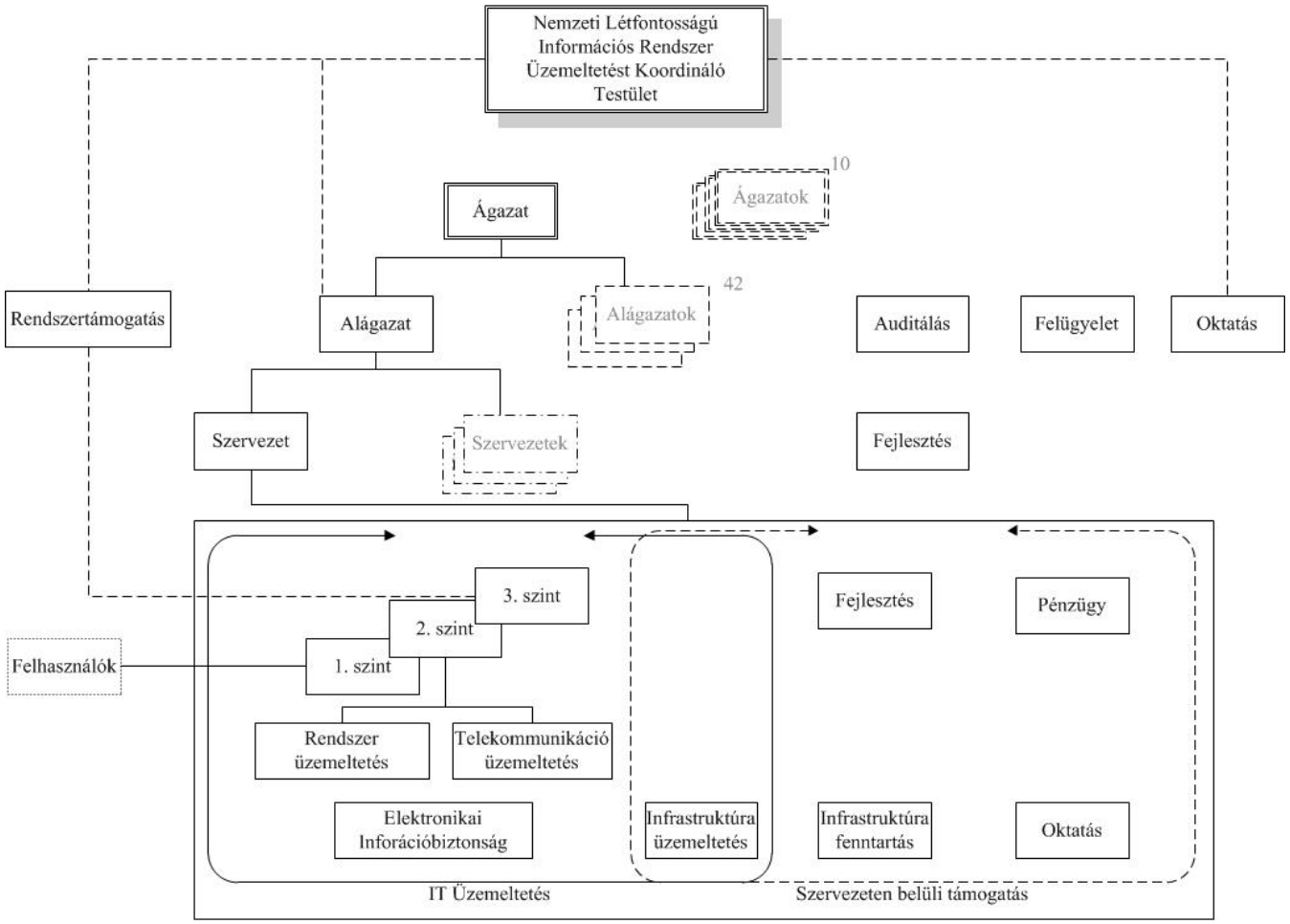
7. táblázat A törvények alkalmazásának alanyai
[19] *3. §,* [55] *II. és III. számú melléklet,* [22] *1. és 2. számú melléklet,* [18] *2. § (1) alapján*

4. SZÁMÚ MELLÉKLET KÜLSŐ FENYEGETETTSÉGEK (EMBERI TEVÉKENYSÉGEK)

Funkció		ELFOGÁS, FELFEDÉS		BEFOLYÁSOLÁS, TÖNKRETÉTEL					
Biztonsági jellemző		Bizalmasság sérül		Adatok sérülékenysége nő Szolgáltatások elérhetősége csökken					
Forma		Közvetett	Követlen	Közvetett			Követlen		
Támadó tevékenység		Információ források felderítése		Megtévesztés	Zavarás	Pusztítás	Megtévesztés	Zavarás	Pusztítás
Támadási szint:	Tudati dimenzió	Viselkedési formák, befolyásolhatóság figyelésével következtetés a döntési folyamatokra	Párbeszédek, döntési folyamatok figyelése HUMINT módszerekkel	Döntéshozatal, megértési folyamat befolyásolása PSYOPS tevékenységekkel (szórólapok, média, internet alkalmazása)			Titkos műveletekkel beszivárgás a célközönség közé és ott a megértési folyamatot befolyásoló témák terjesztése		
	Információs dimenzió	Monitorok kisugárzásának felfedése Hálózati topológia feltérképezése Titkosítás megfejtés, dekódolás	Elektronikai felderítő szenzorok alkalmazása Számítógép hálózatok adataihoz való rejtett hozzáférés, Jelszólopók telepítése	Megtévesztő e–mail üzenet továbbítása Megtévesztő hálózati tevékenység folytatása	Hálózatok adatokkal való mesterséges túlterhelése (Flood Attack), Nyílt forrású információkkal a figyelem elterelése		Trójai programok bejuttatása megtévesztő tevékenység útján Működő programokkal adatok módosítása	Rosszindulatú szoftverekkel, programokkal (férgek, vírusok stb.) hálózati szolgáltatásokhoz való hozzáférés megakadályozása (DDoS), adatok, adatbázisok tönkretétele	
	Fizikai dimenzió	Vezetékes vonalak induktív módon való lehallgatása Papírhulladék kutatása	Információs eszközök, titkosító kulcsok, fizikai kulcsok, adattároló hordozók ellopása	Social Engineering	Bomlasztó tevékenységek előidézése a felhasználók		Fizikai biztonságot feltörve, titkos adatokhoz való hozzáférés	Információs infrastruktúrák fizikai rombolása Infokommunikációs eszközök elektronikai pusztítása.	

8. táblázat Külső fenyegetettségek [25] *92. o.;* [9] *118.o.*

5. SZÁMÚ MELLÉKLET SZERVEZETI FELÉPÍTÉS



11. ábra Javasolt szervezeti felépítés
(saját szerkesztés)

6. SZÁMÚ MELLÉKLET PILAR-TOOLS

test console

SW.std.os HW.pc Media.electronic.disk

SW.std.os HW.pc
SW.std.os HW.pc Media.electronic.disk

threat	frequency	step	[A]	[I]	[C]	[Auth]	[Acc]
[N.1] {D} Fire	0.1	15d	100%				
[N.2] {D} Water	0.1	7d	50%				
[N.*] {D} Other natural disasters	0.1	20d	100%				
[I.1] {D} Fire	0.5	15d	100%				
[I.2] {D} Water	0.5	7d	50%				
[I.*] {D} Other industrial disasters	0.5	15d	100%				
[I.3] {D} Environmental pollution	1	7d	50%				
[I.4] {D} Electromagnetic pollution	1	2d	10%				
[I.5] {D} Hardware or software failure	1	7d	50%				
[I.6] {D} Power interruption	1	1d	100%				
[I.7] {D} Unsuitable temperature or humidity conditi...	1	20d	100%				
[I.10] {D} Media degradation	1	20d	100%				
[I.11] Electromagnetic emanations	1				1%		
[E.1] {D} User errors	1	1h	1%	10%	10%		
[E.2] {D} System / Security administrator errors	1	6h	20%	20%	20%		
[E.8] {D} Malware diffusion	1	1d	10%	10%	10%		
[E.15] Accidental alteration of the information	1			1%			
[E.18] {D} Destruction of information	1	1d	100%				
[E.19] Information leaks	1				10%		

12. ábra PILAR-tools [209] *48. o.*

7. SZÁMÚ MELLÉKLET FENYEGETETTSÉGEK

Típusok	Fenyegetések
Fizikai károk	Tűz
	Vízkár
	Szennyeződés
	Nagy kiterjedésű, vagy súlyosabb baleset
	Eszköz, vagy adathordozó megsemmisülése
	Por, korrózió, fagyás
Természeti események	Rendkívüli, szélsőséges klíma
	Rendkívüli szeizmikus hatás, földrengés
	Vulkánkitörés
	Rendkívüli időjárás
	Árvíz
Kritikus szolgáltatások kimaradása	Légkondicionáló vagy vízellátó rendszer meghibásodás
	Áramkimaradás
	Telekommunikációs eszköz meghibásodása
Sugárzás okozta zavarok	Elektromágneses sugárzás
	Hősugárzás
	Elektromágneses impulzus
Információ kompromittálódása	Áthallásból adódó jelek felfedése
	Távoli kémkedés (kiber tevékenység)
	Lehallgatás
	Adathordozó, vagy dokumentumokeltulajdonítása
	Eszközök eltulajdonítása
	Selejtezett, vagy újrahasznosított adathordozó eredetei adatainak helyreállítása
	Védendő információ nyilvánosságra hozatala, illetéktelennek történő átadása
	Nem megbízható forrásból származó adat
	Hardverelem nem kívánt módosítása
	Szoftver nem kívánt módosítása
	Pozíció bemérése
Technikai meghibásodás	Eszköz meghibásodása
	Eszköz hibás működése
	Szoftver hibás működése
	Információs rendszer karbantartásának elmaradása, rossz végrehajtása

Típusok	Fenyegetések
Engedély nélküli tevékenységek	Eszközök jogosulatlan használata
	Nem jogtiszta szoftver használata
	Hamis vagy másolt szoftverek használata
	Sérült, megváltoztatott adatok használata
	Jogtalan adatfeldolgozás
Funkciók lehetséges veszélyei	Hibás használat
	Jogosultsággal való visszaélés
	Más jogosultságának használata
	Műveletek megtagadása
	Hozzáférés megtagadás

9. táblázat Fenyegetettségek [76] *C melléklet 39-40. o.*

8. SZÁMÚ MELLÉKLET KOCKÁZAT ELEMZÉS TÁBLÁZATAI

			Vagyonelem										
			Épületek			Hardverek			Szoftverek			...	
			Szerverterem_1	Gépház_1	Munkaterem1	Szerver_1	Router_1	NAS_1	Op.rendszer1	Mentőszoftver	Végpontvédelem	...	Kritikussági érték
Munkafolyamatok	Munkafolyamat1		100	100	0	40	20	10	10	0	0	40	320
	Munkafolyamat2												0
		Munkafolyamat_2.1	0	80	20	20	30	20	20	0	0	20	210
		Munkafolyamat_2.2	40	20	10	60	30	10	40	20	10	40	280
		Munkafolyamat_2.3	20	30	20	80	0	0	20	30	20	0	220
	Munkafolyamat3												0
		Munkafolyamat_3.1	40	100	10	40	60	20	20	100	10	10	410
		Munkafolyamat_3.2	40	20	10	30	100	90	0	0	0	30	320
	...		20	10	20	40	20	10	20	30	20	90	280
Kritikussági érték			260	360	90	310	260	160	130	180	60	230	

3. táblázat Folyamat/Vagyonelem függőség szemléltetés

(saját szerkesztés)

		Vagyonelem										Kritikussági érték
		Épületek			Hardverek			Szoftverek			...	
		Szerverterem_1	Gépház_1	Munkaterem1	Szerver_1	Router_1	NAS_1	Op.rendszer1	Mentőszoftver	Végpontvédelem	...	
Veszélyforrások	Tűz	8	3	1	6	1	6	3	8	0	3	39
	Vízkár	4	7	4	4	1	2	0	2	0	0	24
	Szennyeződés	0	3	0	1	1	2	0	1	0	3	11
	Nagy kiterjedésű, vagy súlyosabb baleset	1	3	0	1	1	2	3	4	0	2	17
	Eszköz, vagy adathordozó megsemmisülése	3	0	0	3	1	8	1	7	2	0	25
	Por, korrózió, fagyás	1	4	0	2	1	2	0	2	0	2	14
	Vulkánkitörés	0	1	0	1	1	2	0	0	0	1	6
	Rendkívüli időjárás	2	7	0	2	1	2	0	6	0	2	22
	Árvíz	5	7	0	6	1	5	0	4	2	4	34
Kritikussági érték		24	35	5	26	9	31	7	34	4	17	

4. táblázat Veszélyek/Vagyonelem függőség szemléltetés

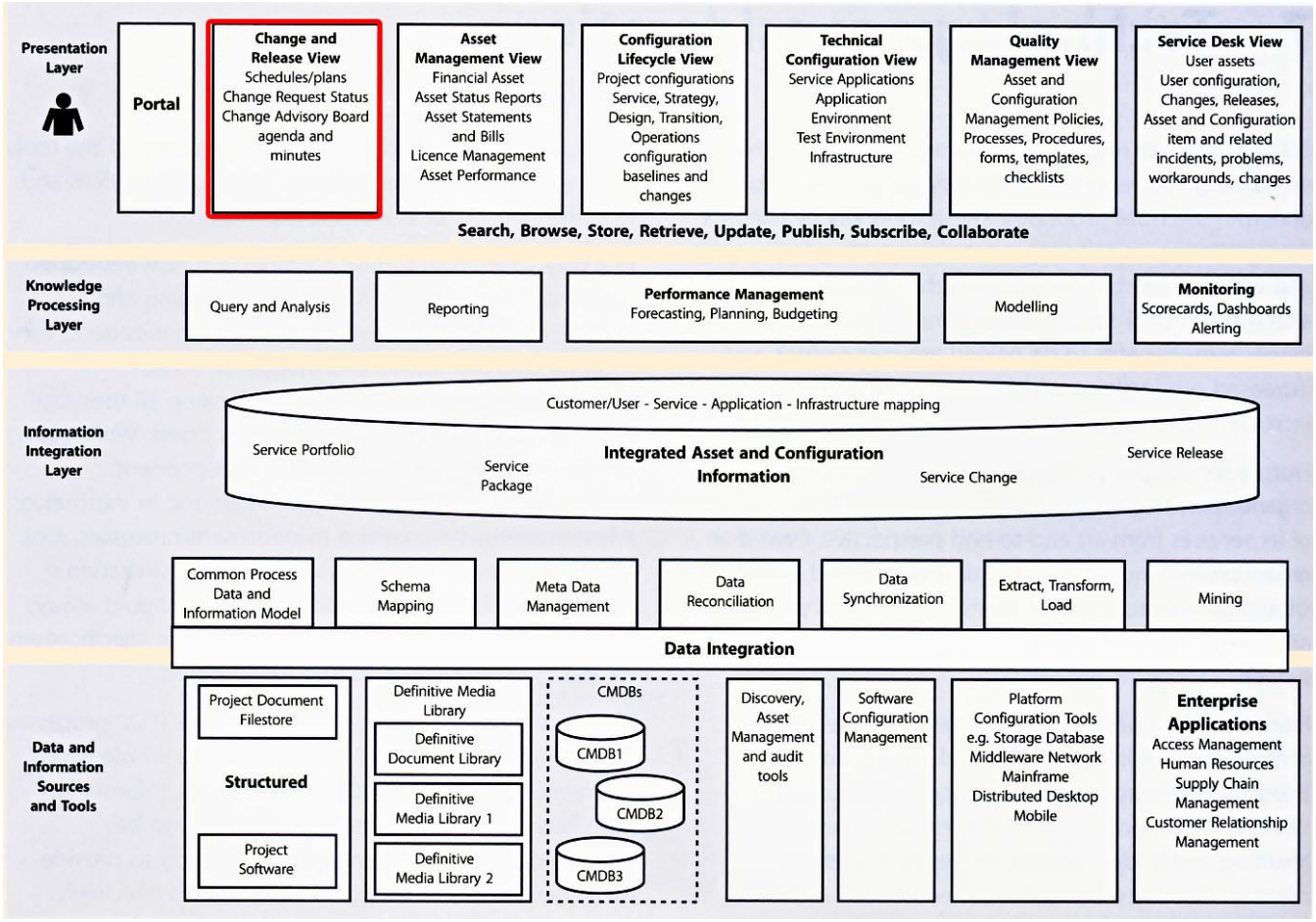
(saját szerkesztés)

		Vagyonelem																				
		Épületek						Hardverek						Szoftverek						...		
1-800		Szerverterem_1		Gépház_1		Munkaterem1		Szerver_1		Router_1		NAS_1		Op.rendszer1		Mentőszoftver		Végpontvédelem		...		Kritikussági érték
801-1600		Értéke (1-300)																				
1601-2400		299		101		40		180		90		240		120		300		280		10		
Veszélyforrások	Tűz	8	2392	3	303	1	40	6	1080	1	90	6	1440	3	360	8	2400	0	0	3	30	8144
	Vízkár	4	1196	7	707	4	160	4	720	1	90	2	480	0	0	2	600	0	0	0	0	3977
	Szennyeződés	0	0	3	303	0	0	1	180	1	90	2	480	0	0	1	300	0	0	3	30	1364
	Nagy kiterjedésű, vagy súlyosabb baleset	1	299	3	303	0	0	1	180	1	90	2	480	3	360	4	1200	0	0	2	20	2929
	Eszköz, vagy adathordozó megsemmisülése	3	897	0	0	0	0	3	540	1	90	8	1920	1	120	7	2100	2	560	0	0	6252
	Por, korrózió, fagyás	1	299	4	404	0	0	2	360	1	90	2	480	0	0	2	600	0	0	2	20	2247
	Vulkánkitörés	0	0	1	101	0	0	1	180	1	90	2	480	0	0	0	0	0	0	1	10	857
	Rendkívüli időjárás	2	598	7	707	0	0	2	360	1	90	2	480	0	0	6	1800	0	0	2	20	4057
	Árvíz	5	1495	7	707	0	0	6	1080	1	90	5	1200	0	0	4	1200	2	560	4	40	6366
Kritikussági érték		24	7176	35	3535	5	200	26	4680	9	810	31	7440	7	840	34	10200	4	1120	17	170	

6. táblázat Káralapú számítás

(saját szerkesztés)

9. SZÁMÚ MELLÉKLET CMS



13. ábra CMS [210]

KÖSZÖNETNYÍLVÁNÍTÁS

Köszönetet szeretnék mondani mindazoknak, akik munkámban segítséget nyújtottak: Elsősorban témavezetőmnek Magyar Sándornak és Rajnai Zoltánnak, akik kezdetektől fogva támogatták kutatásomat és irányt mutattak a tudományos élet területén. Ezúton szeretném megköszönni Deliága Ákosnak, aki az adatközpont kiépítésével kapcsolatos hatalmas tudásanyag átadásal elősegítette, hogy a kutatás és munkám során minden részletre kiterjedően feldolgozhassam a terület kérdéseit. Fontos építőelem volt minden egyes tantárgy és azokat oktató tanár, aki a 3 éves képzés alatt segítette munkámat. Természetesen a végső mű nem jöhetett volna létre Farkasné Hronyecz Erikának a segítsége nélkül, aki a számomra adminisztrációs útvesztőben mutatta mindig a kivezető utat. Végül a családomnak, akiktől hosszabb-rövidebb időre elszakított a kutatói munkám és az értekezés összeállítására fordított tevékenységem, de ők mindvégig támogattak a felkészülésemben.