ZRÍNYI MIKLÓS
NEMZETVÉDELMI EGYETEM

PhD értekezés

Schutzbach Mártonné

Az informatikai rendszerek biztonságának kockázatelemzése a védelmi szférában

Témavezetõ:

Dr. Kun István
a Gábor Dénes Fõiskola fõiskolai tanára

Budapest, 2004

Tartalomjegyzék

BEVEZETÉS

Az információk megszerzésére irányuló tevékenység és a megszerzett információk védelme az emberi társadalmakkal együtt alakult ki. A számítógépek megjelenésével, majd a számítógépes hálózatok kialakulásával az információ megszerzése, feldolgozása, továbbítása, tárolása, védelme nagymértékben megváltozott. Az Egyesült Államokban már az 1970-es évek végén megkezdõdött az informatikai biztonsági értékelés követelményrendszerének kidolgozása. A késõbbiekben, több országban hasonló, nemzeti kiadványok jelentek meg, az informatikai hálózatok elterjedésével megfogalmazódott az igény a nemzetközi szinten egyeztetett követelmények kialakítására is. Magyarországon 1996-ban a Miniszterelnöki Hivatal az Informatikai Rendszerek Biztonsági Követelményei címmel egy hazai ajánlást tett közzé [1]. Az informatikai rendszerek biztonságának megteremtése a gyors fejlõdés, a fenyegetõ tényezõk változása és a megfelelõ biztonsági intézkedések bevezetése miatt nehéz feladat és mindig új problémákat vet fel [2].

A 2001. szeptember 11-én történt Amerika elleni terrortámadás arra is rámutatott, hogy az informatikai vezetõknek és a rendszeradminisztrátoroknak fel kell készülniük a legváratlanabb eseményekre is, hangoztatta John Rimmer[1].

Az informatikai rendszerek egyre nagyobb mértékû alkalmazása az elõnyök mellett új veszélyekkel és kockázatokkal jár a NATO szövetségi, a nemzeti és a védelmi szféra infrastruktúrára nézve is. A védelem megvalósítására, a biztonság megõrzésére a NATO rendszerekben többszintû védelmet kell alkalmazni a védendõ rendszerek fontosságának megfelelõen és el kell fogadni azt a helyzetet, hogy nincs tökéletes biztonság [3].

Az EU 2002/43-as határozatában szerepel, hogy az országok indítsanak információs és oktatási kampányokat abból a célból, hogy a számítógépes hálózatok és információ védelmének ismereteit növeljék, támogassák az információbiztonság menedzsmentjének a nemzetközileg elfogadott szabványokon alapuló gyakorlati módszereit.

Az elõzõek figyelembevételével az alábbi következtetéseket vontam le:

1. Az informatikai biztonság problémaköre elõtérbe került, elvi és gyakorlati kérdései is a kutatások napirendjén van.
2. Nemzetközi és hazai szinten is igény van az egyeztetett követelmények kialakítására.
3. Az informatikai biztonság megteremtéséhez fel kell tárni a fenyegetõ tényezõket, hogy védekezni lehessen ellenük. A fenyegetõ tényezõk sokszínûsége miatt a feltárást részletesen több oldalról megközelítve kell elvégezni.

[1] John Rimmer, az amerikai Országos Információgazdasági Hivatal vezérigazgatója. Forrás: IDG News service 2002. 09. 12

4. A tökéletes biztonság elérése illúziónak tûnik, így elõtérbe kerül a kockázatelemzés, amelynek során meghatározandók a védendõ adatok fontossága, értéke. A veszélyek figyelembevételével lehet dönteni a meghozandó intézkedésekrõl, a védelmi szintrõl, amely arányos a védendõ értékkel. Eldöntendõ, hogy az így visszamaradt kockázat elviselhetõ-e, a *nem elviselhetõ maradvány-kockázat* újabb biztonsági intézkedések meghozatalát teszi szükségessé.

Ezek alapján az értekezésem céljául tûztem ki a következõket:

1. Olyan **kockázatelemzési módszereket, módszertanokat tanulmányozok, hasonlítok össze**, amelyeket már sikeresen alkalmaztak az informatikai rendszerek biztonságának elemzésénél, abból a meggondolásból, hogy az erõsségek és a gyengeségek vizsgálatából hasznosítható következtetéseket vonhassak le a fõ cél, a védelmi szféra informatikai rendszereinek vizsgálatára alkalmazható módszer, megvalósításához.
2. **Kidolgozok a védelmi szféra informatikai rendszereire alkalmazható kockázatelemzési módszertant**, ami figyelembe veszi az eddigi hazai és nemzetközi tapasztalatokat, elvárásokat és a védelmi szféra sajátos helyzetét.
3. Továbbá célom **az informatikai biztonságot fenyegetõ tényezõk teljesebb, több részletre kiterjedõ feltárása és rendszerezése**, mivel a kockázatelemzés sikeressége nagy mértékben függ a fenyegetõ tényezõk ismeretétõl.

A kitûzött célok elérése érdekében a kutató munkám során;

- Tanulmányoztam a dolgozat témájával kapcsolatos hazai és nemzetközi szakirodalmat, a biztonságra vonatkozó fõbb nemzetközi szabályozókat, a hatályos jogszabályokat.
- Konzultációt folytattam a Zrínyi Miklós Nemzetvédelmi Egyetem, a Gábor Dénes Fõiskola, a Bolyai János Katonai Mûszaki Fõiskola, a Budapesti Mûszaki és Gazdaságtudományi Egyetem, a Kürt Computer Rendszerház Rt., a Synergon Informatikai Rt., Takarékbank Rt., a Somogy Megyei Katasztrófavédelmi Igazgatóság, a Fõvárosi Polgári Védelmi Igazgatóság szakemberivel az informatikai biztonsággal kapcsolatos kérdésekrõl.
- Konferenciákon vettem részt, egy részrõl azért, hogy az informatikai biztonságról kialakított elképzeléseim minél nagyobb nyilvánosságot kapjanak és a véleményeket, megállapításokat a további munkámban figyelembe vegyem, másrészrõl a konferenciák megállapításait, irányzatait hasznosíthassam.
- Vizsgáltam a szakirodalomban elõforduló, leggyakoribb kockázatelemzési módszereket, törvényszerûségeket tártam fel, levonható következtetéseket és hasznosítási lehetõségeket soroltam fel.
- Elemeztem a kockázatkezelésnél alkalmazott matematikai módszerek lehetõségeit.

- A védelmi szféra egy területének informatikai rendszerét vizsgáltam, és a kidolgozott kockázatelemzési módszer néhány lépését alkalmaztam.
- Értékeltem kutatásaim, tapasztalataim és megfigyeléseim eredményeit.

Az értekezésem felépí tése:

- A **bevezetésben** a téma kidolgozásának motivációit sorolom fel, megfogalmazom a célokat, az alkalmazott módszereket.
- Az **elsõ fejezetben** az informatikai biztonság megteremtésének lehetõségével foglalkozom, áttekintem a biztonságra vonatkozó fõbb nemzetközi szabályozókat, hatályos jogszabályokat, biztonsági szabványokat. Kiemelem a védelmi szféra informatikai biztonságának sajátosságait. Vizsgálom az informatikai rendszerek életciklusának hatását a biztonságra.
- A **második fejezetben** a kockázatelemzési módszerek vizsgálatával, összehasonlításával arra a kérdésre keresem a választ, hogy a nagyszámú kockázatelemzési módszert hogyan lehet alkalmassá tenni, kiegészíteni, vagy ilyen eljárást kialakítani egy adott informatikai rendszerre történõ alkalmazáshoz. Ez a fejezet tartalmaz egy sajátos matematikai módszert, a fuzzy elmélet felhasználhatóságát a kockázatkezelésben.
- A **harmadik fejezet** módszertani útmutatót ad a védelmi szféra informatikai rendszereinek kockázatelemzéséhez. Tartalmazza a kockázatelemzés egyes lépéseinél használható eszközöket, amelyek a kapcsolattartást, az áttekinthetõséget, az informatikai rendszer, a szervezet megismerését, a fenyegetõ tényezõk feltárását segítik. Lényegesnek tartottam a kockázatelemzés egyes lépéseinek a gyakorlatban való megvalósíthatóságának bemutatását. Az értekezésnek nem célkitûzése, így nem is tartalmazza a védelmi szféra egy konkrét informatikai rendszerének teljes kockázatelemzését.
- A **negyedik fejezetben** az informatikai rendszer egyes részterületeit, mint a környezeti infrastruktúra, az alkalmazások, a rejtjelezés és a hálózatok problémakörét vizsgálom. A fenyegetõ tényezõk, a gyengepontok feltárása a sikeres kockázatelemzés egyik alappillére, így ebben a fejezetben is elõkerül az egyes területek veszélyhelyzeteinek felmérése.
- Az **ötödik fejezet** tartalmazza az eredmények összegzését, következtetések levonását, az értekezés felhasználhatóságának elemzését, a további kutatási irányok felvetését.
- A **hivatkozott és felhasznált irodalom** interneten található Web lapokra való hivatkozásokat is tartalmaz. Az itt szereplõ internet címeket 2003. október 26.-án mûködõképesnek találtam.

Végül köszönetet mondok mindazoknak, akik munkájukkal, javaslataikkal segítették az értekezésem elkészítését.

1. Az informatikai biztonság megteremtése

Ebben a fejezetben azoknak az informatikai biztonsághoz tartozó fogalmaknak a pontos jelentését írom le, amelyeket a dolgozatomban a megadott értelemben használok. A továbbiakban röviden ismertetem az informatikai biztonsággal kapcsolatos fontosnak tartott jogszabályokat, szabványokat és ajánlásokat. A szabványok és ajánlások általános és ismételten alkalmazható megoldásokat adnak fennálló vagy várható problémákra és általában elõírásaik alkalmazása a legkedvezõbb hatással jár az adott tevékenységre vagy termékre nézve.
A biztonsági követelmények kidolgozásának az a célja, hogy az intézmények vezetésének és a területen dolgozó szakértõknek információt nyújtsanak a szervezetek informatikai biztonságának megteremtéséhez.

1.1. Alapfogalmak

Biztonság:
A biztonság olyan feltételek, körülmények megteremtése és szavatolása jogszabályokkal, állapotvédelmi erõkkel, eszközökkel, alkalmazási technológiákkal és módokkal, amelyek a törvényes rend megsértésére érzékeny vagy a veszélyes helyzetekben minimálisra csökkentik a bizonytalansági és kockázati tényezõket. Megfelelõ védelmet nyújtanak a természetszerû vagy szándékos veszélyt keltõ hatások ellen, azzal, hogy azokat idõben felfedik, hatásmechanizmusukat akadályozzák, gyengítik, kioltják, azaz összességében õrködnek a létrehozott biztonsági *állapot* szintjének megtartásán. A biztonság komplex kategória, amelyen belül a katonai tényezõkön túl elõtérbe kerültek más összetevõk (pl. politikai, gazdasági, társadalmi, emberjogi – esetleg kisebbségi –, környezeti és informatikai) is.
Az információ- és az informatikai biztonság:
Az információbiztonság az adatok által reprezentált információ sértetlenségét, bizalmasságát, rendelkezésre állását biztosítja, ezen belül az informatikai biztonság az informatikai rendszer által kezelt és tárolt adatok által hordozott információk körére vonatkozik és vizsgálódási területe az adatokon kívül az összes rendszerelem, amelyek valamilyen kapcsolatban vannak az adatokkal. Az Informatikai és Hírközlési Minisztérium fogalomtára az informatikai biztonságot az információs rendszer tulajdonságaként értelmezi, ez a tulajdonság a rendszer biztonsági követelményeinek és céljainak teljesülését mutatja. Az 1. számú melléklet szemlélteti az informatikai biztonság helyét a NATO biztonsági rendszerében.
Védelem:
A védelem olyan tevékenység, illetve olyan *tevékenységek sorozata*, amely arra irányul, hogy megteremtse, folyamatosan szinten tartsa és fejlessze a biztonságot. Az angol security szó tartalma biztonságvédelem, a biztonság megóvását, biztosítását jelenti. A

2. számú melléklet a veszélyelemzés szemszögébõl közelíti meg a biztonságvédelem területeit.

Az 1992. évi LXIII. törvény - a személyes adatok védelmérõl és a közérdekû adatok nyilvánosságáról - egyértelmûen kettéválasztotta az adatvédelem és az adatbiztonság fogalmát, ez alapján a továbbiakban a két fogalmat a következõképpen használom:

Adatbiztonság (data security):

Az adatok védelme a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetõleg sérülés vagy a megsemmisülés ellen.

Adatvédelem (data protection):

Az adatvédelem magában foglalja a személyes adatok védelmét, valamint a közérdekû adatok megismeréséhez való jog érvényesülését szolgáló alapvetõ szabályokat.

Az információtechnológia (a továbbiakban IT) **rendszerelemei:** az informatikai biztonság körébe tartozó adatok kezelését, tárolását, továbbítását végzõ eszközök, erõforrások összessége.

IT rendszer: az IT rendszerelemek és kapcsolataik összessége.

Kockázat: A kockázat az angol *risk* többjelentésû szó fordítása. Egyrészt veszélyt, veszélyforrást jelent, másrészt matematikai valószínûséget. Eszerint objektív illetve szubjektív kockázatról beszélhetünk. A BS 8800 angol szabvány szerint a kockázat a meghatározott veszélyes esemény valószínûségének és következményeinek kombinációja. Matematikai értelemben a kockázat úgy definiálható, mint adott idõ alatt a rendszert ért váratlan eseményekbõl keletkezõ kár várható értéke. A kockázatokat több szempont szerint osztályozhatjuk, pl. az azonosíthatóság, elfogadhatóság, felismerhetõség szerint, ez utóbbi alapján beszélhetünk nyilvánvaló vagy rejtett kockázatról.

Kockázatelemzés:

A rendelkezésre álló rendszer-információ módszeres és tudatos felhasználása a veszélyek azonosítására, a kockázat meghatározására.

Az értekezésemben a kockázatelemzés folyamatát egy összetettebb folyamat, a kockázatkezelés részének tekintem, a rendszerben való elhelyezkedést az 1.1. ábrán szemléltettem. [4]

Kockázatkiértékelés:

A kockázat elfogadhatóságának kiértékelése.

Kockázatértékelés:

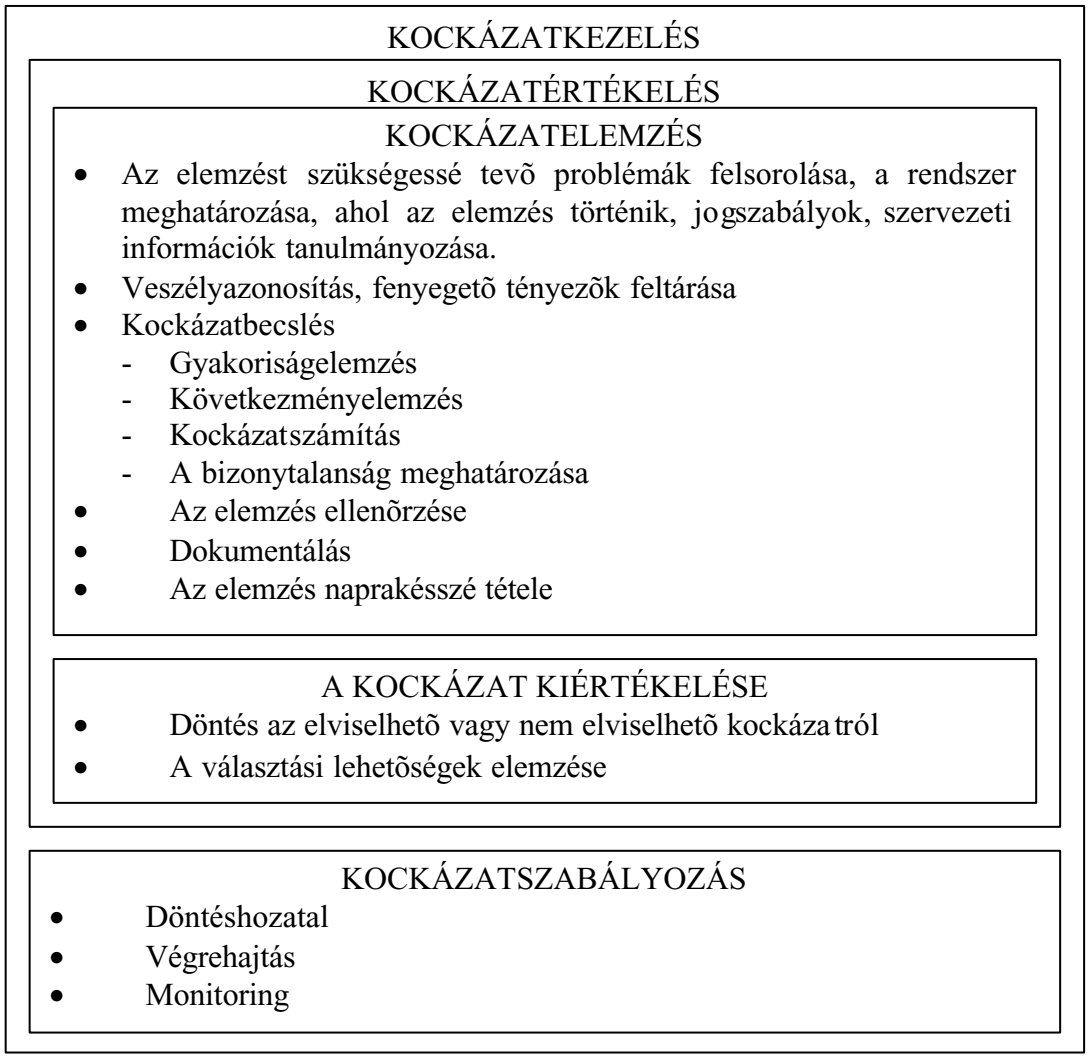
A kockázatelemzési és kockázatkiértékelési folyamatok együttese.

Kockázatszabályozás:

A kockázatok kezelésével összefüggõ döntéshozatali folyamat; a döntések végrehajtása és rendszeres felülvizsgálata.

Kockázatkezelés:

A kockázatelemzési, a kockázatkiértékelési és kockázatszabályozási feladatokkal kapcsolatos elvek, eljárások és a gyakorlat módszeres alkalmazása.



1.1. ábra. A kockázatkezelés rendszere

1.2. Az informatikai biztonságra vonatkozó fõbb nemzetközi ajánlások, hatályos jogszabályok, biztonsági szabványok áttekintése

A védelmi intézkedéseknél különbözõ szabályozási szinteket kell figyelembe venni.

1. szint: törvények, jogszabályok
2. szint: mûszaki normák, szabványok, rendeletek
3. szint: ágazati szintû végrehajtási utasítások
4. szint: helyi szabályzatok

1.2.1. Az informatikai biztonsági átvilágítás kialakítása során figyelembe veendõ fontosabb jogszabályok

- 1995. évi LXV. törvény az államtitokról és a szolgálati titokról, a végrehajtására kiadott 79/1995. (VI. 30.) sz. Kormány rendelet.

- 1992. évi LXIII. törvény a személyi adatok védelmérõl és a közérdekû adatok nyilvánosságáról.
- 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról.
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.
- 1998. évi LXXXV. törvény a Nemzeti Biztonsági Felügyeletrõl. „A NBF részletes feladatairól és mûködési rendjérõl, valamint az iparbiztonsági ellenõrzések részletes szabályairól" szóló 52/2002. (III.26.) sz. Kormány rendelet, továbbá „A nemzetközi kötelezettségvállalás alapján készült minõsített, valamint a korlátozottan megismerhetõ adat védelmérõl" szóló 56/1999. (IV. 4.) sz. Kormány rendelet.
- Magyarország NATO csatlakozásakor kötelezettséget vállalt, a NATO Biztonsági Szabályzatában [C-M (2002) 49 (Final)] leírtak szerint, a minõsített NATO-adatok védelmére. A Nemzeti Biztonsági Felügyelet, az 1998. évi LXXXV. törvény alapján, dönt a biztonsági garanciát jelentõ tanúsítványok kiadásáról is. A NATO-szabályzat elõírásokat tartalmaz a minõsítési eljárásokról, a minõsített információk védelmérõl, a NATO minõsített információk ipari környezetbe történõ kihelyezésének szabályairól. Az 1998. évi LXXXV. törvény kiegészítette a Nemzetbiztonsági Szolgálatokról szóló 1995. évi CXXV. törvénynek a Nemzetbiztonsági Hivatal, illetve a Katonai Biztonsági Hivatal feladatait.
- Az EU biztonsági szabályzata, 2001/264 Council Decision on security regulations.

1.2.2. A szabványokról

A XX. század elején jöttek létre a fejlett európai országokban a nemzeti szabványügyi szervezetek. A nemzetközi kereskedelem kialakulása vezetett a nemzetközi szabványügyi szervezetek létrehozásához, így beszélhetünk nemzetközi, regionális és nemzeti szabványokról. Pl.:

ISO[2], IEC[3]	nemzetközi szabványok	alkalmazásuk önkéntes
EN[4]	regionális szabványok	alkalmazásuk önkéntes
MSZ[5], DIN[6]	nemzeti szabványok	alkalmazásuk önkéntes
Vállalati szabványok	egy adott vállalaton belül kötelezõen alkalmazandók	

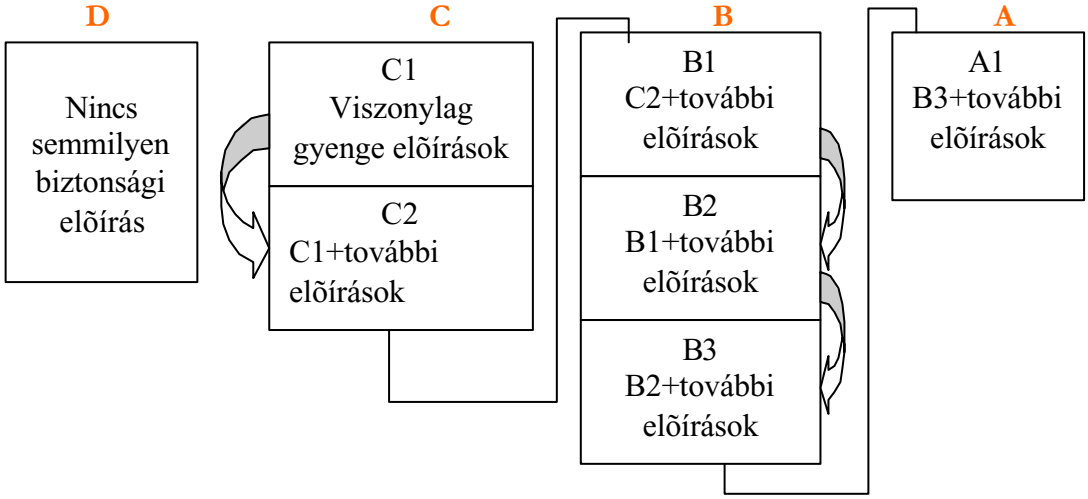
A téma kidolgozásánál hasznos információkat nyújtó szabványokat az 3. számú melléklet tartalmazza.

[2] ISO: Nemzetközi Szabványosítási Szervezet (International Standards Organization)
[3] IEC: Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission)
[4] EN: Európai Szabvány (Europäische Norm)
[5] MSZ: Magyar Szabvány
[6] DIN: Német Szabványügyi Intézet (Deutsches Institut für Normung)

1.2.3. Ajánlások, követelmények

TCSEC: (Trusted Computer System Evaluation Criteria = Biztonságos Számítógépes Rendszerek Értékelési Kritériumai = orange book). Az Egyesült Államok informatikai biztonsággal kapcsolatos követelményrendszere, a kormányzati és katonai rendszerek alkalmazásában kötelezõ. A TCSEC négy csoportot és ezen belül biztonsági osztályokat határoz meg. Az osztályok egymásra épülnek:

A1 > B3 > B2 > B1 > C2 > C1 > D.



1.2. ábra. A TCSEC biztonsági osztályai

D csoport: minimális védelem

Ezek a rendszerek bárki számára szabadon használhatók, módosíthatók, esetleg törölhetõk.

C csoport: szelektív és ellenõrzött védelem

C1 osztály: korlátozott hozzáférés-védelem

A felhasználók a jogosultságuknak megfelelõ tevékenységet végezhetnek a rendszerben.

C2 osztály: nem szabályozott, de ellenõrzött hozzáférés-védelem

Az elõzõnél szigorúbb, mert a jogosultsággal rendelkezõ felhasználót a rendszeradminisztráció azonosítja.

B csoport: kötelezõ és ellenõrzött védelem

B1 osztály: címkézett és kötelezõ hozzáférés-védelem

A rendszer objektumai (hardver, szoftver, adatok, felhasználók stb.) a hozzáférési mechanizmust szabályozó címkével ellátottak.

B2 osztály: strukturált hozzáférés-védelem

A rendszer objektumainak azonosítása és a hozzáférés ellenõrzése elkülönített referenciamonitor használatával történik.

B3 osztály: elkülönített védelem

Az egyes objektumokat fizikailag és logikailag is elkülönítik egymástól, az ide tartozó rendszerek az egyes területeket elkülönítve kezelik.

A csoport: bizonyí tott védelem

A1 osztály:

A B3 osztály kitételein túl, követelmény a biztonsági rendszer eredményes mûködésének matematikai bizonyítása is.

ITSEC: (Information Technology Security Evaluation Criteria =Információtecnoló gia Biztonsági Értékelési Kritériumai). Az Európai Közösség országaiban ezt a követelményrendszert széles körben elfogadják és használják a potenciális felhasználók és piaci szektorok. Az ITSEC hét biztonsági szintet határoz meg, ezeket E0, E1, E2, E3, E4, E5, E6- tal jelöli, és rendre megegyeznek a TCSEC D, C1, C2, B1, B2, B3, A1 osztályokkal. Az ITSEC tíz funkcionalitási osztálya:

F-C1:

Korlátozott hozzáférés- védelem.

F-C2:

Korlátozott és ellenõrzött hozzáférés- védelem, a hozzáférési jogokat csoportoknak vagy egyes személyeknek határozzák meg.

F-B1:

Címkézett kötelezõ hozzáférés- védelem.

F-B2:

Strukturált hozzáférés- védelem.

F-B3:

Elkülönített védelmi területek.

F-IN:

Nagy integritású rendszerek osztálya; az azonosítás, a hitelesítés, a jogkezelés, a jogellenõrzés és a bizonyításos biztonság követelményeinek kell megfelelnie a sértetlenség (integritás) szempontjából.

F-AV:

Magas rendelkezésre állást igénylõ rendszerek osztálya; egy rendszer hozzáférhetõségét kell nagy biztonsággal megvalósítani.

F-DI:

Adatmozgatásnál magas adatintegritást biztosító rendszerek osztálya; az adatcserénél kell a hitelesítés, az átvitel- biztosítás és bizonyításos biztonság segítségével elérni a magas szintû informatikai biztonságot.

F-DC:

Bizalmas adatokat feldolgozó rendszerek osztálya; az adatkezelésnél nagy mérvû titoktartást kell biztosítani.

F-DX:

Magas adat- integritást és bizalmasságot biztosító osztott rendszerek osztálya; az ilyen rendszerek nyilvános nem védett hálózatokhoz kapcsolódnak, és ehhez biztosítanak magas szintû titkosságot és sértetlenséget.

CC: (Common Criteria =Közös Követelmények) Az Európai Közösség, az USA és Kanada együttmûködésével jött létre abból a célból, hogy a korábbi ajánlásokat összhangba hozza és a különbözõ alkalmazási területekre egyedi követelményeket szabjon. A COMMON CRITERIA (CC) 1.0 verziója 1996-ban jelent meg, az informatikai rendszerek és termékek biztonsági értékelésével foglalkozik. A bõvített 2.0-ás verziót 1998 áprilisában adták ki, 1999-ben ebbõl készült az ISO 15408-as szabvány. Apróbb változtatások után 1999 augusztusában bevezetésre került a ma is érvényben lévõ CC 2.1-es verzió.

Az informatikai biztonság területén rendkívüli jelentõséggel bíró ISO/IEC 15408 szabványhoz hazánk képviseletében az Informatikai és Hírközlési Minisztérium 2003. szeptember 19-én csatlakozott.

A nemzetközi egységesítési törekvések célja volt az egységes és általánosan elfogadott fogalomrendszer, az elvárások, a módszertanok kialakítása. A CC felhasználja az elõzõ követelményrendszerek fogalmait (TCSEC, FC[7], CTCPEC[8], ITSEC), de új fogalmakat is bevezet, és egy egészen más szemléletet mutat.

Az informatikai rendszerek biztonságának megteremtése magában foglalja

- a számítástechnikai eszközöket és rendszereket,
- az informatikai rendszerek környezetét,
- az informatikai rendszerrel kapcsolatba kerülõ személyeket,
- a rendszerekre, az üzemeltetésre vonatkozó szabályozásokat, elõírásokat, dokumentumokat.

A CC megnevezi azokat a biztonságot érintõ fenyegetettségeket, amelyek a rendszert veszélyeztethetik, különválasztva azokat, amelyeket az IT rendszernek vagy a környezetnek kell kivédenie, így pontosan behatárolhatók a felelõsségek határai.

A CC meghatározások:

IT biztonsági értékelés: az IT termék vagy rendszer biztonsági tulajdonságaira vonatkozó módszeres vizsgálat. A vizsgálat eredménye egy nyilatkozat, amely az adott rendszer biztonsági szintjére utal.

Védelmi profil: egy termék-független megközelítés. A CC által megadott és formalizált követelményekbõl egy adott feladatot lefedõ követelményrendszer építhetõ fel. Egy feladatra több védelmi profil készíthetõ, ha különbözõ fenyegetõ tényezõket vagy körülményeket vesznek figyelembe. A felhasználó választhat, hogy az elõre elkészített védelmi profilok közül melyik közelíti meg legjobban az adott körülményeket. Ha nem talál, a mindig bõvülõ profilok között neki megfelelõt, akkor megrendelheti vagy elkészítheti azt. Az új profilt értékeltetni kell, vele szemben szigorú formai elõírások vannak. Tartalmaznia kell a veszélyek leírását; a CC húsz fenyegetettségi osztályt, ezen

[7] FC: Az Információtechnológia Biztonságára vonatkozó Szövetségi Kritériumok (Federal Criteria for Information Technology Security)

[8] CTCPEC: Kanadai Megbízható Számítástechnikai Termékek Minõsítési Követelményrendszere (Canadian Trusted Computer Product Evaluation Criteria)

belül 106 fenyegetettséget határoz meg, ezek kiegészíthetõk az adott rendszer sajátos tényezõivel.

Egy védelmi profil a következõ részeket tartalmazza:

- A bevezetõben van a profil rövid leírása, amely segíti a felhasználót a választásban.
- Az informatikai rendszer vagy termék, azaz az értékelés tárgyának leírása.

A vizsgált rendszer biztonsági környezetének leírása három fõ területre irányul, a fenyegetések, a belsõ szabályzatok és eljárások, a rendszer fizikai és személyi környezetével szembeni igények leírására.

- A biztonsági célok meghatározása (a rendszerre és környezetére vonatkozóan).
- A biztonsági követelmények meghatározása, ami jelenti a rendszer biztonsági követelményeinek, az elérendõ biztonsági osztály, valamint az IT környezet biztonsági követelményeinek a leírását.
- Indoklás; a benne megfogalmazott állítások igazolják a biztonsági osztály kiválasztását, hogy minden ismert fenyegetõ tényezõt figyelembe vesznek, a kitûzött célok mindenben megfelelnek a jogszabályi követelményeknek, a funkcionális követelmények lefedik a biztonsági célokat, a biztonsági követelmények összefüggõek és ellentmondás-mentesek.

Biztonsági rendszerterv; termékfüggõ dokumentum, a védelmi profilban leírtakat konkrét megoldási módokra fordítja le.

A CC a biztonsági követelményeket funkcionális és garancia csoportokra osztja:

A *biztonsági funkciókat* a következõ osztályokba csoportosítják;

- biztonsági naplózás,
- kommunikáció, felhasználói adatok védelme,
- azonosítás, hitelesítés,
- magántitok,
- a biztonsági funkciók megbízható védelme,
- erõforrás-hasznosítás,
- az informatikai rendszerekhez való hozzáférés,
- megbízható csatornák.

Az osztályokat tovább bontják családokra, a családokat komponensekre.

Garanciakövetelmények (a vizsgálatokkal szembeni elvárások):

Hasonlóan a funkcionális osztályokhoz a garanciaosztályok is családokra, a családok pedig komponensekre oszlanak.

A garanciaosztályok a következõk; konfiguráció-kezelés, szállítás, mûködtetés, fejlesztés, útmutató dokumentumok, életciklus-támogatás, tesztek, sebezhetõség felmérése.

Garanciaszintek azt mutatják meg, hogy az informatikai rendszer vagy termék vizsgálatát milyen mélységben, milyen erõforrás ráfordítással végezték, magasabb garanciaszinteken nagyobb költségráfordítással vizsgálták az informatikai rendszert. A CC hét garanciaszintet különböztet meg;

- funkcionálisan tesztelt,
- strukturálisan tesztelt,
- módszeresen tesztelt és ellenõrzött,
- tervszerûen tervezett, tesztelt és áttekintett,
- félformálisan tervezett és tesztelt,
- félformálisan igazoltan tervezett és tesztelt,
- formálisan igazoltan tervezett és tesztelt

A CC a védelmi profil fogalmának bevezetésével és ilyen profilok kidolgozásával segítséget ad a felhasználóknak, akik a megfelelõ védelmi profil kiválasztásával *külsõ segítség nélkül* megvizsgálhatják, hogy az informatikai rendszerük vagy egy termékük megfelel-e a biztonsági szempontoknak. Az IT termékek fejlesztõi, gyártói is profitálhatnak ebbõl a megközelítési módból, mert ismert védelmi profilhoz illeszkedve fejleszthetnek termékeket. Az informatikai rendszert értékelõk a meghatározott feltételek szerint véleményezik, hogy az informatikai rendszer vagy termék kielégíti-e a követelményeket.

A CC-ben nagy hangsúlyt kap az informatikai rendszer teljes életciklusa alatti követelmények vizsgálata, amely kiterjed a tervezés, elõállítás és fejlesztés menetére is. Így az elkészült, nagyon bonyolult informatikai rendszerek vizsgálata után kisebb a valószínûsége annak, hogy rejtett hibák maradnak a rendszerben.

INFOSEC: Information Systems Security - informatikai rendszerek biztonsága

A NATO információvédelemmel kapcsolatos ajánlása, amely szerint „Az információvédelem biztonsági intézkedések alkalmazása annak érdekében, hogy a kommunikációs, információs és más elektronikus rendszerekben tárolt, feldolgozott és átvitt adatok védelme biztosítva legyen a bizalmasság, sértetlenség és rendelkezésre állás elvesztésével szemben, függetlenül az események szándékos vagy véletlen voltától.” Az INFOSEC tevékenységi céljai:

bizalmasság	sértetlenség	rendelkezésre állás
Az adatok bizalmasságának megvédése, annak garanciája, hogy az adatokhoz jogosulatlanul vagy illetéktelenül nem juthatnak hozzá.	Az adatok sértetlensége (integritása) azt jelenti, hogy azokat csak az arra jogosultak változtathatják meg.	Annak a biztosítása, hogy az adatok mindig elérhetõek legyenek, jogtalanul ne semmisítsék meg, ne töröljék azokat.

Az INFOSEC két fõ része:

Communication Security (COMSEC): a kommunikációs biztonsággal foglalkozik.

Három fõ területe:

CRYPTOSEC - CRYPTOgraphic SECurity - rejtjelezés

TRANSEC - TRANSmission SECurity - az átviteli utak védelme

EMSEC - EMission SECurity - a kompromittáló kisugárzás elleni védelem

Computer Security (COMPUSEC): a számítógépes rendszerek biztonságát vizsgálja, azaz

- Hardverbiztonság: Az intézkedések akkor teljes körûek, ha a teljes infrastruktúrára kiterjednek.
- Szoftverbiztonság: A logikai védelem biztonsági követelményeinek teljesülése.
- Firmware-biztonság: A firmware-biztonság azt jelenti, hogy a csak olvasható memóriában tárolt programot használó eszközök, részegységek funkciójuknak megfelelõen mûködnek, a támadásokkal szemben védettek.

Egy másik felfogás szerint az INFOSEC területei:

- COMSEC (CRYPTOSEC, TRANSEC, EMSEC)
- Computer security
- LAN security
- Intercommunication of Network security

ITB ajánlások:

A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága[9] által kiadott ajánlások az informatikai biztonság megteremtésének legfontosabb tudnivalóiról adnak tájékoztatást.

ITB 8. számú ajánlás; tartalmazza az informatikai biztonság kockázatelemzésének egy jól használható módszertanát.

ITB 12. számú ajánlás; az informatikai rendszerek biztonságának követelményeit tartalmazza.

ITB 16. számú ajánlás; az informatikai termékek és rendszerek biztonsági értékelésének módszertana.

---

[9] A **Kormány 3296/1991. (VII.5.)** határozata értelmében a koordinálandó feladatok tartalmi körének meghatározásával létrejött a Miniszterelnöki Hivatal (MeH) közigazgatási államtitkár irányítása alatt 1991.november 27-ei alakuló üléssel az **Informatikai Tárcaközi Bizottság** és annak munkaszervezete, a MeH szervezeti keretei között az **Informatikai Koordinációs Iroda.**

1999 júniusáig a Miniszterelnöki Hivatalban az informatikai és kormányzati távközlési ügyekben illetékes helyettes államtitkár irányította a kormányzati információpolitika kidolgozását, a Hivatal feladat- és hatáskörébe utalt informatikai, kormányzati távközlési tevékenységeket, és hangolta össze az ezekkel kapcsolatos központosított közbeszerzési feladatokat. A helyettes államtitkárság szerepét 2000 júniusától az **Informatikai Kormánybiztosság** vette át.

Az ITKTB, vagyis az Információs Társadalom Koordinációs Tárcaközi Bizottság a kormány 1214/2002. (XII.28) sz. határozata alapján alakult meg 2003. február 25-én, az Informatikai és Hírközlési Minisztériumban. Az ITKTB elfogadta a **M**agyar **I**nformációs **T**ársadalom **S**tratégiát, és a kormánynak elfogadásra javasolta a tervezetet., a MITS 2003. októberében megjelent.

Az ITB biztonsági osztályai:

- *Alapbiztonsági osztály*: A személyi adatok, a pénzügyi adatok, az üzleti titkok, egy szervezet belsõ szabályozása által meghatározott korlátozás alá esõ adatok, a nyílt adatok feldolgozására alkalmas rendszerek biztonsági osztálya.
- *Fokozott biztonsági osztály*: A szolgálati titok, a nem minõsített különleges személyes adatok, a nagy tömegû személyes adat, a banktitkok, a nem nagy értékû üzleti titkok feldolgozására alkalmas rendszerek biztonsági osztálya.
- *Kiemelt biztonsági osztály*: Az államtitok, a katonai szolgálati titok, a nagy tömegû különleges személyes adat, a nagy értékû üzleti titkok feldolgozására alkalmas rendszerek biztonsági osztálya.

A fenti osztályok minimális követelményeinek részletes felsorolását az 4. számú melléklet tartalmazza.

1.2.4. Kapcsolat a különbözõ biztonsági osztályok és szintek között

TCSEC	ITSEC	ITB 12. ajánlás		
A1	F-B3; E6			
B3	F-B3; E5			
B2	F-B2; E4			KIEMELT
B1	F-B1; E3		FOKOZOTT	
C2	F-C2; E2	ALAP		
C1	F-C1; E1			
D	E0			

Mivel nincs egységesített biztonsági osztály-besorolás[10], ezt az összehasonlítást meg kell tenni, mert elõfordulhat, hogy egy adott informatikai rendszer rendszerelemei mindegyike más biztonsági minõsítéssel rendelkezik, vagy nincs minõsítése. Amennyiben egy védelmi tervhez az egységesítésre szükség van, akkor az egy ilyen táblázat használatával lehetséges.

Vizsgáljuk meg, hogy egy rendszert hogyan lehet besorolni egy biztonsági kategóriába!

NCSC eljárás: (NCSC = National Computer Security Center által kidolgozott eljárás)

- Meg kell határozni a rendszer ún. kockázati indexét. A kockázati index olyan érték, amely egyrészrõl annál nagyobb minél bizalmasabb adatok találhatók a rendszerben, másrészrõl minél kisebb jogú felhasználója lehet a rendszernek.
- A kockázati index meghatározásához szükséges az adatok bizalmasságának értéke, ezt egy nyolc fokozatú skálán adjuk meg, az R_{max} mérõszámmal fejezzük ki. (0=tetszõlegesen hozzáférhetõ; 7=szigorúan titkos)

[10] ITB 12. sz. ajánlás (Informatikai rendszerek biztonsági követelményei) is tartalmaz összehasonlító táblázatot. Az ajánlás szerint a kiemelt biztonsági osztály tartalmazza a TCSEC B3 osztály néhány követelményét is.

- A legkisebb jogú felhasználó jogkörét az R_{min} számmal jellemezzük, amely szintén 0-tól 7-ig vehet fel értékeket. (0=semmi joga nincs; 7=minden joga megvan)
- A kockázat indexet a következõképpen képezzük:

kockázati index	**Feltétel**
R_{max}-R_{min}	ha Rmin < Rmax
1	$R_{min} \geq R_{max}$, de vannak olyan adatok, amelyekhez nem mindenki férhet hozzá
0	Egyébként

- A rendszer számára kívánatos minimális biztonsági kategóriát ezt követõen a kockázat indexbõl határozhatjuk meg:

kockázat index	kategória nyílt biztonságú rendszer	kategória zárt biztonságú rendszer
0	C2	C2
1	B1	B1
2	B2	B2
3	B3	B2
4	A1	B3
5	*	*
6	*	*
7	*	*

Nyílt biztonságú rendszer azt jelenti, hogy nem lehet kizárni a lehetõségét annak, hogy a rendszer fejlesztõi vagy karbantartói avatkoznak a rendszerbe rossz szándékkal. Zárt biztonságú rendszer esetén ez kizárható.

A *-gal jelzett esetekben a kívánt biztonságot nem lehet elérni csak információ-technikai védelemmel, hanem további (fizikai, adminisztratív, stb.) eszközökre is szükség van.

A következõ táblázat a biztonsági alapfunkciók osztályonkénti megjelenését és eloszlását mutatja. (ITB 12, 1996 ajánlása szerint)

Jelmagyarázat:

	nincs követelmény az adott osztályban,
	új vagy bõvített követelmény jelenik meg az adott osztályban
	nincs újabb követelmény az adott osztályban

Osztály	Biztonsági alapfunkciók									
	Információvédelem							Megbízható mûködés		
	I+A	DAC	MAC	ACC	AUD	DAT	TFM	AV	TRE	FUN
B3										
B2										
B1										
C2										
C1										

- I+A: azonosítás és hitelesítés (Identification and Authentication),
- DAC: szabad belátás szerint kialakított hozzáférés-vezérlés (Discretionary Access Control),
- MAC: elõre meghatározott hozzáférés-vezérlés (Mandatory Access Control),
- ACC: jogosultság ellenõrzés, elszámoltathatóság (Accountability),
- AUD: biztonsági vizsgálat (Audit),
- DAT: biztonságos adatcsere (Data Exchange). Itt csak a rejtett csatornákra vonatkozó követelményeket vettük figyelembe,
- TFM: biztonságos kezelési funkciók (Trusted Facilities Management). A biztonsági felügyelõ, a rendszeradminisztrátor és a felhasználók szerepkörének szétválasztása,
- AV: a rendelkezésre állás biztosítása (Availability),
- TRE: a biztonságos rendszer-visszaállítás biztosítása (Trusted Recovery),
- FUN: a funkcionalitás biztosítása (Functionality).

Az ITB eljárása:

Meghatározzák a kártípusokat:

- közvetlen anyagi,
- közvetett anyagi,
- társadalmi-politikai, humán,
- személyi sérülés, haláleset,
- jogszabály által védett adatokkal történõ visszaélés vagy azok sérülése.

Kialakítanak egy kárérték osztályozást:

"0": jelentéktelen kár

"1": csekély kár

"2": közepes kár

"3": nagy kár

"4": kiemelkedõen nagy kár

"4+": katasztrofális kár

- **alapbiztonsági** követelményeket kielégítõ informatikai rendszert kell létrehozni akkor, ha a rendszerben maximum "**2**", azaz legfeljebb **közepes kárértékû** esemény bekövetkezése fenyeget,
- **fokozott biztonsági** követelményeket kielégítõ informatikai rendszert kell létrehozni akkor, ha a rendszerben maximum "**3**", azaz legfeljebb **nagy kárértékû** esemény bekövetkezése fenyeget,
- **kiemelt biztonsági** követelményeket kielégítõ informatikai rendszert kell létrehozni akkor, ha a rendszerben a "**4+",** azaz a **katasztrofális kárértékig** terjedõ esemény bekövetkezése fenyeget.

1.3. Az informatikai biztonság létrehozásának lépései

Az informatikai biztonság csak fizikai, eljárás- és algoritmusos védelem együttes alkalmazásával teremthetõ meg.

A FIZIKAI VÉDELEM	ELJÁRÁS-VÉDELEM	ALGORITMUSOS VÉDELEM
1. A hardver és szoftver védelme 2. A helyiségek, objektumok védelme 3. A papír alapú és más hagyományos dokumentumok védelme	Az Informatikai Biztonsági Szabályzat írja le azokat a biztonsági szabályokat, tevékenységi formákat, amelyek az informatikai rendszert üzemeltetõ szervezet ügymenetébe épített védelmi intézkedések	Az információ algoritmusos védelmével a kriptográfia foglalkozik. A kriptográfia többek között a következõ feladatokat látja el; titkosítás, visszafejtés, hozzáférés-védelem, hitelesítés, partnerazonosítás, digitális aláírás, …

1.3.1. Fizikai védelem

A hardverek és szoftverek fizikai védelme több tényezõt foglal magában;

- eltulajdonítás elleni védelmet, vagyonvédelmet,
- mechanikai sérülések elleni védelmet,
- a számítástechnikai eszközök folyamatos mûködésének biztosítását,
- a számítástechnikai eszközök tempest támadás (elektromágneses sugárzás érzékelése) elleni védelmét,
- villámvédelmet,
- szoftverek és adatok védelmét a megfelelõ hozzáférési jogosultságokkal,
- a szoftverekkel kapcsolatban a biztonsági másolatok készítésének, tárolásának problémáját.

Helyiségek, objektumok védelme jelenti;

- az adott helyiségek mozgásérzékelõvel, hõ- és füstérzékelõvel, kamerákkal történõ figyelését,

- õrzésvédelmet, beléptetés - a helyiségekbe belépõ személyek azonosítását, a jogosultságok kezelését,
- kerítés, falak, ajtók, biztonsági tárolók védelmét.

A papír alapú és más hagyományos dokumentumok védelme;

- a hozzáférés-védelem páncélszekrénybe vagy védett helyiségbe való elzárás lehet,
- a biztonság növelésére az aláíráson kívül is vannak eszközök, mint a vonalkód, a dombornyomású bélyegzõ használata, mágnescsík, hologram, optikai pecsét elhelyezése a papírlapon.

1.3.2. Eljárás-védelem

A biztonsági stratégia legfontosabb eleme a szabályozás, amelyre a stratégia összes többi eleme épül. A szabályoknak, szabványoknak és az eljárásoknak egyértelmûvé kell tenni az elvárásokat és a fentiek megsértése esetén a következményeket.
A szabályok arra a kérdésre adnak választ, hogy miért fontos az informatikai biztonság, a szabványok megfogalmazzák, hogy mi az elfogadható szintje a biztonságnak a szabályokban definiált területeken. Az eljárások leírják, hogy hogyan kell megvalósítani a biztonságot növelõ intézkedéseket, hogy azok megfeleljenek a szabályzatokban és szabványokban leírtaknak.

Az informatikai biztonsági koncepció kialakítása:

A koncepciónak tartalmaznia kell az adott szervezet informatikai biztonsággal kapcsolatos elvárásait, a szükséges intézkedéseket, az intézkedések következményeinek vizsgálatát.

Az informatikai biztonsági szabályzat:

Az informatikai biztonsági koncepcióban megfogalmazott intézkedéseket a szervezetre alkalmazható formában, tehát más szabályokkal és a körülményekkel összhangban szabályzattá alakítják.

1.3.3. Algoritmusos védelem

Az informatikai biztonsággal foglalkozó szakirodalom nagy része az algoritmusos védelemmel, azon belül kriptográfiával foglalkozik. A téma népszerûsége azzal magyarázható, hogy már a számítógépek elterjedése elõtt több évszázaddal foglalkoztak a kutatók a rejtjelezés tudományával.

KRIPTOLÓGIA A titkos és védett kommunikáció tudománya	
KRIPTOGRÁFIA	KRIPTOANALÍZIS
Az információk rejtjelezésével foglalkozik.[11]	A rejtjelezett információk feltörésére irányuló eljárásokkal foglalkozik.

A fizikai védelem az informatikai rendszerbe történõ belépési helyeket, az eljárás-védelem a belépési helyek használatának elfogadható, elvárt formáit határozza meg. Az eljárás-védelem összekapcsolja a fizikai védelem területét az algoritmusos védelemmel.

1.4. A védelmi szféra informatikai biztonságának sajátosságai

A biztonságot komplex kategóriaként értelmezem, amelyen belül a katonai tényezõkön túl elõtérbe kerültek pl. a politikai, gazdasági, társadalmi, emberjogi, környezeti és informatikai összetevõk is. A biztonságot veszélyeztetõ tényezõk is sokoldalúak, a védelemnek is annak kell lenni, azaz megszüntetni vagy elfogadható szintre csökkenteni a kockázati tényezõket. Ennek megfelelõen a védelmi szféra magába foglalja a katonai védelmen túl például a rendvédelmet, az önkormányzati védelmet, a gazdaságvédelmet, gazdaságmozgósítást, a külpolitika egyes elemeit, a nemzetbiztonsági szolgálatok tevékenységeit is.
A többféle megközelítést, de mindenekelõtt a *Magyar Köztársaság biztonság- és védelempolitikájának alapelveirõl szóló határozat*[12] definícióját figyelembe véve a védelmi szférára a következõ meghatározást tettem; **mindazon szervezetek és tevékenységek összessége, amelyeknek az elsõdleges feladata a biztonság megteremtése, megtartása.**
A védelmi szféra átfogó terület, így a dolgozatban csak egy-egy rész kiemelésére van lehetõségem, ebben a fejezetben a NATO informatikai rendszereinek biztonságával foglalkozom. A második fejezetben (2.5.) a Vám- és Pénzügyõrség bûnüldözésre és a katonai mûveletek környezetre vonatkozó kockázatelemzése, valamint a NATO kockázatelemzési módszere szerepel. A harmadik fejezet kidolgozott kockázatelemzési módszertana a védelmi szféra informatikai rendszereinek kockázatelemzésére alkalmas, egyes lépéseit a Fõvárosi Polgári Védelmi Igazgatóság informatikai rendszerére alkalmaztam. A fenyegetõ tényezõk feltárását és rendszerezését a védelmi szféra általános területen végeztem el, kiemeltem a védelmi szféra azon sajátosságát, hogy az informatikai rendszereik nagy kihívást jelentenek a támadóknak. A hálózatokon keresztül nagy kárt lehet okozni, idõlegesen megbénítható a gazdaság, a bankrendszer, az egészségügy, a kormány, a rendvédelem, a katonai védelem.

---

[11] 43/1994. (III. 29.) Kormányrendelet a rejtjeltevékenységrõl

[12] "A honvédelem rendszere az Észak-atlanti Szerzõdésbõl fakadó jogok és kötelezettségek egységére, az ország és a Szövetség védelmi igényeit tudatosan elfogadó polgárok önbecsülésére és felelõsségére, a fegyveres erõk és a védelem anyagi szükségleteit kielégíteni képes gazdaságra, a védelemre felkészült államszervezetre, a védelem katonai feladatait ellátni képes fegyveres erõkre, a fegyveres erõk demokratikus és polgári irányítására és ellenõrzésére, a lakosság és az anyagi javak megóvását szolgáló polgári védelemre, valamint a magyar társadalom legszélesebb rétegeinek támogatására épül"-94/1998. (XII. 29.) OGY Határozat A Magyar Köztársaság biztonság- és védelempolitikájának alapelveirõl. 13. pont, 2. bekezdés.

A védelmi szféra egyes területein számítógépes gerinchálózat van kiépítve, amelyen keresztül a lokális hálózatok az információcsere biztonságának figyelembevételével összekapcsolhatók. Problémaként vetõdik fel, hogy a védelmi szféra informatikai rendszerei a kereskedelemben kapható szoftverekbõl és hardverekbõl épülnek fel. Több éve foglalkozik a védelmi szféra azzal, hogy a kereskedelemben kapható, de külön eljárással minõsített és bevizsgált szoftverekkel kell az informatikai feladatokat megoldani. A nyílt rendszerek irányába történt már elmozdulás. Az internet kapcsolat a minõsített adatokat tartalmazó rendszerek számára tilos, a nem minõsített adatokat tartalmazó rendszerek tûzfalak alkalmazásával kapcsolódhatnak egymáshoz és a nyilvános rendszerekhez.

Az informatikai rendszerek biztonságának védelme a NATO-ban [5] :

A NATO-ban a védelem alapja a *minõsítés*. A 8. számú melléklet az 1995. évi LXV. törvény az államtitokról és szolgálati titokról 2003 júliusi módosításából a NATO-ra vonatkozóan lényeges kiemeléseket tartalmaz.

A védelemmel kapcsolatos új követelmények:

- Az informatikai rendszereknek jobban meg kell felelniük a mûveleti követelményeknek, már az alacsonyabb stratégiai fontosságú szinteket is védeni kell.
- A védelmet több információ cseréjére kell felkészíteni.
- A védelmet az erõk áthelyezése, mobilitása esetén javítani és fejleszteni kell.

A NATO tevékenységeinek három szintjét kell alapul venni az informatikai biztonság kialakításában; a politikai, a mûveleti és az információtechnológiai szintet.

Az informatikai biztonsággal kapcsolatos feladatok a politikai szinten:

- Információ biztosítása a vezetési-irányítási rendszerek számára a kutatás és fejlesztéshez, a doktrínához, a szabványokhoz és a kiképzéshez.
- Politikai szinten kell koordinálni a NATO tagországok megfelelõ nemzeti szervezeteiben a törvények végrehajtásának, a rejtjelezés szabályozásának, az információtechnológia alkalmazásának, az export ellenõrzésének és a felderítési információk megosztásának védelmét.
- A nem katonai információs infrastruktúráért felelõs nemzeti szervezetek tevékenységének koordinációja.
- A NATO tagországok törvényeinek és szerzõdéseinek koordinációja.
- A felderítési és riasztási információk cseréjének koordinálása.

Az informatikai biztonsággal kapcsolatos feladatok az információs mûveletek szintjén:

Információs mûveletek; az információszerzés, a védelem és a támadás.

Az informatikai biztonság magában foglalja:

- A technikai biztonságot, ami kiterjed a kisugárzás, a továbbítás, a megbízható adatfeldolgozás, a hálózat és a rejtjelezés biztonságára.
- A nem technikai biztonságot (mûveleti biztonság, fizikai biztonság).

Az informatikai biztonsággal kapcsolatos feladatok az információtechnológia szintjén:
Minden felhasználói kapcsolatfelvétel esetén szükséges a hozzáférés és a jogosultság ellenõrzés, a rejtjelezés. Ehhez a következõket kell betartani;

- minden objektum címkézése, abból a célból, hogy a hozzáférést naplózni lehessen,
- minden hozzáféréssel rendelkezõ személy, valamint a szoftver azonosítóval való ellátása,
- minden akció módszeres vizsgálata, nyomkövetési lehetõséggel,
- azoknak a hardvereknek és szoftvereknek a fokozott védelme, amelyek ezeket a feladatokat megvalósítják.

A NATO tagországok számára az INFOSEC ad egységes útmutatásokat a kommunikációs és a számítógépes biztonság megteremtéséhez.

1.5. Az informatikai rendszerek életciklusának hatása a biztonságra

Az informatikai rendszerek életét a létrehozásról szóló döntéstõl a rendszer mûködésének megszüntetéséig a következõ szakaszokra bonthatjuk; elõkészítés, tervezés, megvalósítás, üzemeltetés, üzembõl történõ kivonás. Az informatikai biztonsági rendszerekre is érvényes az életciklus modell. A megvalósítást és üzemeltetést elõ kell készíteni, meg kell tervezni, majd a megvalósítás után üzemeltetni, ellenõrizni, tovább fejleszteni kell a rendszert, az üzembõl történõ kivonásnak két fontos lépése van; a szükséges adatok mentése és a eszköz megsemmisítése, visszaminõsítése.
Az informatikai rendszerek nem biztonságos mûködésének valószínûsége idõvel növekszik. Az üzembe helyezés pillanatában bizonyos, hogy a rendszer biztonsága elfogadható, amennyiben gondos elõkészítés és tervezés elõzte meg. Ahogy telik az idõ, a biztonság fokozatosan csökken a következõ auditig. Ha a felülvizsgálatot megfelelõ kockázatmenedzselés követi, akkor a rendszer ismét biztonságosnak mondható.
A szervezetek informatikai rendszere folyamatosan változik, egy-egy komponens elavul és helyére új technológia kerül. Ahhoz, hogy a szervezeti biztonsági szint megközelítõleg konstans legyen, folyamatosan ellenõrizni kell a rendszereket.

1.6. Összegzés

Az alapfogalmak pontos meghatározása nehéz feladat, mivel ezeket a köztudatban esetleg más-más értelemben vagy kissé módosított jelentéssel használják. Így az elsõ fejezetben célszerûnek láttam definiálni a biztonsággal kapcsolatos fogalmakat, amelyeket a továbbiakban az itt megadott értelmezésben használok. Az informatikai rendszerek biztonságának megteremtését a magas szintû jogszabályok, a nemzetközi és nemzeti ajánlások, a különbözõ szabványok, intézményi szabályozások hierarchikus rendje teszi lehetõvé, ezért tanulmányoztam a fõbb jogszabályokat, szabványokat, a különbözõ ajánlásokat és összefoglaltam az egységesítési lehetõségeket a biztonsági osztályok között. Az informatikai biztonság célja az informatika rendszer olyan

állapotának elérése, amelyben a kockázatokat elfogadható szintre csökkentették fizikai, eljárás- és algoritmusos védelem együttes alkalmazásával.
A védelmi szféra vezetése, irányítása állandó döntéshozatali tevékenységet folytat, amihez elengedhetetlenek az információs mûveletek. A nagy mennyiségû információ megszerzése, tárolása, feldolgozása, továbbítása magas követelményeket támaszt a védelmi szféra informatikai rendszereivel és a rendszerek biztonságával szemben.

2. Kockázatelemzési módszerek vizsgálata, összehasonlítása

Az informatikai rendszerek biztonságos mûködésének értékeléséhez, ismernünk kell a rendszer zavarainak kockázatát. Tudnunk kell, hogy milyen károkat szenvedhet el a szervezet a tárolt vagy feldolgozott adatok, illetve az azokat támogató erõforrások valamilyen sérülése esetén. Ha az adatok, a feldolgozásukhoz, megjelenítésükhöz szükséges erõforrások nem állnak rendelkezésre, vagy esetleg illetéktelen kezekbe kerülnek, akkor ez magas helyreállítási költségeket, helytelen döntéseket, jogi következményeket, bizalomvesztést, esetleg részleges vagy teljes mûködésképtelenséget vagy más problémákat vonhat maga után. Ezért szükséges a kockázatelemzés és az elemzés következményeképpen a kockázatok kezelése.
Az 1970-es években fejlesztették ki az IBM-nél informatikai kockázatelemzésre a Courtney[13] eljárást, Európában a 80-as évek közepén kezdtek kockázatelemzési módszertanokat kidolgozni, a 90-es években a legismertebb az Angliában forgalomba hozott CRAMM, és a Franciaországban elterjedt MARION[14] eljárás volt.
Az általános kockázatelemzés egy részterülete az informatikai kockázatelemzés, amely alatt az informatikai rendszert, az informatikai infrastruktúrát és az ezeket üzemeltetõ informatikai szervezetet fenyegetõ veszélyek rendszeres azonosítását, vizsgálatát és értékelését értjük. A nagy nemzetközi informatikai elemzõ cégek (pl.: Gartner Group, International Data Corporation) felmérései azt mutatják, hogy Nyugat-Európában és Észak-Amerikában fokozatosan elõtérbe került a kvantitatív kockázatelemzés, a lehetséges informatikai kockázatok számszerûsítése. Az elõre megadott kockázati skálán való értelmezés és ábrázolás szemléletesebbé teszi az informatikai rendszerben történõ változtatások, javítások szükségességét. A kvalitatív kockázatelemzés során nem valószínûségeket, biztonsági mérõszámokat állapítanak meg, hanem súlyossági és kockázati szinteknek egy fogalmi meghatározását adják.
A kockázatelemzéseket deduktív és induktív eljárásokként is csoportosíthatjuk. A deduktív eljárásoknál egy végeseményt feltételeznek és az elõidézõ okokat keresik. Az induktív eljárásoknál egy rendszerelem-meghibásodást feltételeznek, és az elemzés

[13] A Courtney módszer: Két tényezõ, a bekövetkezés várható gyakorisága és az esemény bekövetkezésekor fellépõ anyagi kár nagysága, áll ennek az eljárásnak az elõterében. A két tényezõ szorzata adja az eredõ kockázat várható értékét.

[14] MARION eljárás: Méthodologie d' Analyse des Risques Informatiques et d' Optimisation par Niveau

során rögzítik azokat az eseményeket, amelyeket ez a rendszerelem-meghibásodás okozhat.
Az elsõdleges célom a kiválasztott öt módszer elemzésével és összehasonlításával, hogy a védelmi szféra informatikai rendszereinek kockázatelemzésére alkalmas eljárást találjak vagy készítsek a levont tapasztalatok alapján.

2.1. Kockázatelemzési módszertanok

2.1.1. CRAMM

A CCTA Risk Analysis and Management Method az Egyesült Királyság CCTA (Central Computer and Telecommunications Agency) szervezete által alkalmazott kockázatelemzési és menedzselési módszertan.
A CRAMM kockázatkezelésének fõ lépései:

I. A védelmi igény feltárása	1. Az informatikai alkalmazások és a feldolgozandó adatok felmérése
	2. Az informatikai alkalmazások és a feldolgozandó adatok értékelése
II. Fenyegetettség-elemzés	3. A fenyegetett rendszerelemek felmérése
	4. Az alapfenyegetettség meghatározása
	5. A fenyegetõ tényezõk meghatározása
III. Kockázatelemzés	6. A fenyegetett rendszerelemek értékelése
	7. A károk gyakoriságának meghatározása
	8. A kockázat meghatározása
IV. Kockázatkezelés	9. Az intézkedések kiválasztása
	10. Az intézkedések értékelése
	11. A költség/haszon arány elemzése
	12. A maradvány-kockázat elemzése

I. A védelmi igény feltárása: kiválasztják a szervezet lényeges informatikai rendszereit, az informatikai alkalmazásokat, amelyeket védeni akarnak.
II: Fenyegetettség-elemzés: azoknak a fenyegetõ tényezõknek a feltárása, amelyek az elõbbi adatokra, alkalmazásokra veszélyesek lehetnek.
III. Kockázatelemzés: a fenyegetõ tényezõk hatását vizsgálják az informatikai rendszerre, meghatározzák a lehetséges károk bekövetkezésének gyakoriságát és a kárértékeket.
IV: Kockázatkezelés: a megfelelõ intézkedések kiválasztása és értékelése a károk csökkentésére.
A CRAMM kockázatkezelési folyamatának részletezése a 5. számú mellékletben található.

A CRAMM módszertan nagy elõnye, hogy a feladatokat következetesen, lépésrõl lépésre leírja, így a kockázatkezelés gyakorlati megvalósításához sok segítséget ad.
A szakaszok felépítése;

- a szakasz áttekintése,
- a szakasz elõzménye,
- a szakasz eredménye,
- kapcsolódási pontok,
- a szakasz lebonyolítása.

A lépések leírásának felépítése;

- áttekintés,
- segédletek,
- résztvevõk,
- eredmény,
- kapcsolódási pontok,
- lebonyolítás.

A CRAMM módszertan táblázatai a konkrét feladatnak megfelelõen bõvíthetõk, jó támpontot adnak a kockázatkezeléshez.

2.1.2. ITB. 8. számú ajánlás

A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága által 1994-ben kiadott informatikai biztonsági módszertani kézikönyv.
Az ITB 8. számú ajánlás a brit kormány informatikai központja (CRAMM -CCTA Risk Analysis and Management Method) és az északrajna-vesztfáliai kormány informatikai központja kormányzati informatikai biztonsági dokumentumainak (Informationtechnik Sicherheitshandbuch - KBSt 1991) felhasználásával készült. Az ITB ajánlások tanulmányozhatók az Informatikai Tárcaközi Bizottság honlapján (http://www.itb.hu).

2.1.3. COBIT

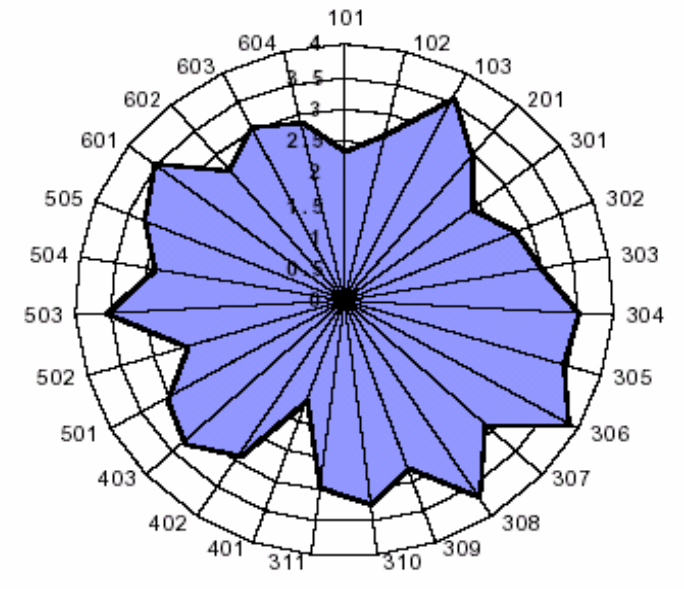
A COBIT (Control Objectives for Information and related Technology) egy nyílt szabvány, irányelveket tartalmaz az információtechnológia alkalmazásával összefüggõ kontrollrendszer kialakításához és ellenõrzéséhez. Az IT szabványok, a jól bevált módszerek és gyakorlatok egységes rendszerbe foglalt módszertana. Ez a módszertan segítséget ad egy rendszer terveinek, irányelveinek, szabályozásainak, valamint informatikai szervezetének felépítéséhez, és a folyamatos mûködés biztosításához is.
A COBIT fõ részei:

- Vezetõi összefoglaló (Executive Summary), felsõ vezetõknek
- Szerkezet (Framework), vezetõknek, azaz informatikai, biztonsági és belsõ ellenõrzési szervezeti egységek vezetõinek

- Irányítási feladatok (Control Objectives), középvezetõknek, azaz informatikai, biztonsági és belsõ ellenõrzési szervezeti egységek középvezetõinek
- Auditálási elvek (Audit Guidelines), folyamatvezetõknek, ellenõrzési szakembereknek
- Megvalósítási eszközkészlet (Implementation Tool Set), informatikai, biztonsági és belsõ ellenõrzési igazgatóknak, középvezetõknek, menedzsereknek.

2.1.4. MARION eljárás

A MARION négy szakaszból áll, amelyek közül az egyiket az elsõ szakasz elé írhatnánk be, mint elõkészítõ fázist. Az elõkészítõ szakasz egy olyan szervezet felépítését írja le, amelynek a továbbiakban a kockázatelemzést kell kivitelezni. Az elemzés minõsége erõsen függ ennek a teamnek az összeállításától. Az elsõ szakaszban egy *gyengepont-elemzést* végeznek azáltal, hogy egy átfogó katalógus általános és különleges biztonsági szituációkra vonatkozó kérdéseit megválaszolják. Ezekre a kérdésekre egy skála alapján, egy saját belátás szerinti bevezetendõ egységben adják meg a választ és különbözõen súlyozzák. Az eredményeket megfelelõ grafikonon ábrázolják. Ezt a gyengepont-elemzést a kockázat-felismerés technikájának tekintik. További kockázat-felismerési technikaként szolgál a második szakasz *kockázat-scenarioinak elemzése*. Itt vitatják meg a kockázati helyzetek összes lehetséges következményeit, beleértve a valószínûség becslését és a kár mértékét. A harmadik szakasz a *biztonsági intézkedések tervezésével* foglalkozik.
A módszer legnagyobb elõnye a vizsgált terület biztonsági állapotának nagyon szemléletes ábrázolása. A 27 biztonsági tényezõ értékelése egy rozetta sugarain belülrõl kifele történik, ez a rozetta valójában a statisztikában közismert sugárdiagram. A 0 jegy, amely a középpontban van, kevés vagy kicsi, a 4-es jegy a külsõbb körön nagyon jó vagy akár teljes védelmet jelent.
Egy durva felosztással a rozetta jobb oldala az általános ellenõrzést, a társadalmi és gazdasági tényezõk valamint az általános fizikai biztonsági aspektusokat reprezentálja, a baloldal ezzel szemben a logikai biztonságot, tehát a hardver, a szoftver és a termék és rendszerfejlesztés biztonságát.
A következõ illusztráció egy vizsgált rendszer biztonsági állapotát szemlélteti és mutatja; például a 301 (fizikai környezet) terén intézkedések bevezetése szükséges, mivel csak 2,4 –es jegyet kapott, ezenkívül felhívja magára a figyelmet a 401 (hardver és rendszer biztonság) az 1,6-es jeggyel. A vizsgálat során nagyon pozitív megítélést kapott a 103 (biztonsági eljárások és audit), a 306 (vízvédelem), 308 (katasztrófa elhárítási folyamatok) vagy az 503 (biztonsági másolat) témakör.



2.1. ábra. MARION rozetta

A MARION eljárás, amely Európa szerte elterjedt, az Európai Unióban is használják számos sajátos eszközzel támogatott.

2.1.5. IT-Grundschutzhandbuch

Egy IT kézikönyvet 1992-ben a BSI[15] publikált Németországban, IT- Sicherheitsbuch címen, átdolgozás és gyakorlatiasabbá tétel után kapta az alapvédelmi kézikönyv címet, amit 1995-ben adtak ki.

Ebben a biztonsági kézikönyvben olyan eljárást írtak le, amelynek segítségével egy informatikai rendszer biztonságának megállapítása és az IT biztonság garantálása lehetséges. Az eljárás négy fokozatban - a védelmi igény meghatározása, veszélyelemzés, kockázatelemzés és az IT biztonsági koncepció elõkészítése - összesen tizenkét lépésbõl áll.

A módszer célkitûzése:

- Egy IT-rendszernél olyan biztonsági szint elérése, amely alacsony és közepes védelmi szükséglet számára alkalmas és elegendõ.
- Kiinduló alapul szolgálni a magas védelmi igényû felhasználóknak is.

Tehát nagyon fontos a meggyõzõ és egyértelmû védelmi igény megállapítása. A célkitûzésnek megfelelõen a módszer csak alacsony és közepes védelmi igény esetén alkalmazható közvetlenül. Az eljárás olyannyira részletezett, hogy ez alapján minden további segítség nélkül végigvezethetõ. A módszer egy olyan építõjátékhoz hasonlít, amely 27 építõ kockából áll. Minden egyes építõkockához egy veszélyhelyzet és egy megfelelõ intézkedés tartozik.

[15] BSI: Bundesamt für Sicherheit in der Informationstechnik

A „veszélykatalógus” öt fõcsoportot tartalmaz:

G1: magasabb kényszer

G2: szervezeti hiányosság

G3: emberi hibák

G4: technikai hiba

G5: szándékos cselekedetek

Az intézkedéseket hat fõkategóriába foglalták össze:

M1: infrastruktúra

M2: szervezet

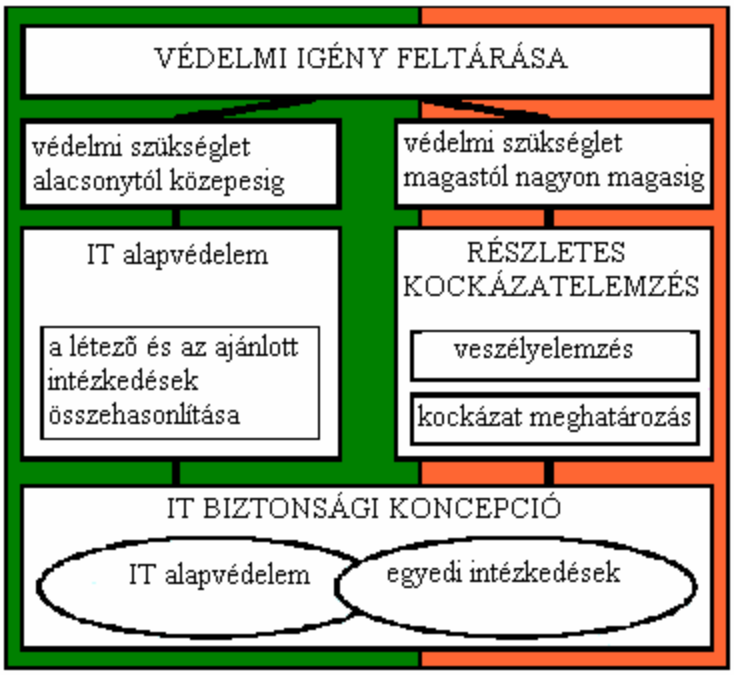
M3: személyzet

M4: hardver és szoftver

M5: kommunikáció

M6: katasztrófa megelõzés

Az IT rendszereket, amelyek a megfelelõ védelmi igény meghatározás szerint az IT alapvédelem felhasználására alkalmasak, az építõkockákkal és az ajánlott intézkedésekkel a lehetõ legpontosabban lefedik



2.2. ábra. Az IT-Grundschutzhandbuch biztonság-kialakításának lépései

2.2. Kockázatelemzési módszerek összehasonlítása

Az értekezésem egyik célkitûzése - kockázatelemzési módszerek összehasonlítása. Ebben a fejezetben indoklom a módszerek kiválasztásának szempontjait, felsorolom az egyes eljárások pozitívumait és negatívumait. Az összehasonlításhoz mind mennyiségileg, mind tartalmilag megfelelõ összehasonlító kritérium szükséges, az összehasonlítási szempontok kiválasztásánál a saját elképzelésem mellett figyelembe vettem a szokásos elvárásokat, a különbözõ biztonsági szakemberek véleményét, a szakirodalomban elõforduló, módszertanokkal szembeni követelményeket. A vizsgált módszerek összehasonlító szempontok szerinti értékelését grafikus megjelenítéssel teszem szemléletesebbé.

Az összehasonlításban a CRAMM, az ITB 8. számú ajánlása, a COBIT, a MARION és az IT-Grundschutzhandbuch szerepel. *A kiválasztásnál a következõ szempontokat vettem figyelembe:*

- Az informatikai biztonság témakörét hazánk uniós csatlakozása miatt célszerû az Európai Unió tagországaiban vizsgálni.
- Az összes létezõ ajánlás, módszer, módszertan vizsgálata helyett a legismertebbeket választottam ki, így a francia MARION-t, a német IT-Grundschutzhandbuch-t, egy nemzetközi szervezet által létrehozott COBIT-ot, az angol CRAMM-et és végül, de egyáltalán nem utolsó sorban a ITB 8. számú ajánlást, mivel Magyarországon ezt az ajánlást minden informatikai biztonsággal foglalkozó szervezet ismeri és egészében vagy kiindulási alapként felhasználja.

CRAMM elõnyei és hátrányai:

- A CRAMM átfogó megközelítés a kockázatelemzés és kezelés feladatkörére.
- Szoftverrel és jól használható sablonnal támogatott.
- Számos intézkedést ajánl a kockázatok csökkentésére.
- Eszközt nyújt szükséghelyzetekben is.
- Az eljárás ösztönzi az elemzõket az informatikai rendszer egy alapos biztonsági auditjának elvégzésére.
- A CRAMM –nak több verziója is megjelent, ezek közül egy magyar fordításban is. A CRAMM CCTA Risk Analysis and Management Methodology, Guidance on CRAMM for Management, Version 2.0, CCTA, February 1991 ismert nálunk is. 2003-ban az ötödik verziónál tartunk.
- Nagyon nagy körben használt módszer (a NATO is használja) így már sok tapasztalati tényezõt beépítettek.
- Kockázatelemzése alapos, részletes, segítségével a kockázatok mindig meghatározhatók.

- Ezzel szemben fellépnek bizonyos hátrányok is; ezen módszer szerinti kockázatelemzés hosszadalmas, így költséges, a kockázatok nem határozhatók meg egzaktul, az eredmények gyorsan túlhaladottakká válnak.
- Egy rendszer teljes elemzése ezzel a módszerrel hónapokat is igénybe vehet, így gyakran csak a gyakorlott felhasználók vagy az eljárás kivitelezésére szakosodott csoportok tudják alkalmazni.

ITB 8. számú ajánlás elõnye és hátrányai:

- 1994-ben adta ki az Informatikai Koordinációs Iroda az ITB 8. számú ajánlását, az Informatikai Biztonsági Módszertani Kézikönyvet, 1994 óta újabb verzió nem jelent meg.
- Ez a módszer a német, északrajna-vesztfáliai Informationtechnik Sicherheitshandbuch-ján és a brit kormány által használt CRAMM módszeren alapul. A felhasznált német és az angol módszertan kiállta a gyakorlat próbáját.
- A módszertant közel tíz éve használjuk a gyakorlatban, kezdetben államigazgatási szervezetek auditálására, de a késõbbiekben a legelterjedtebb módszertanná vált az informatikai biztonság vizsgálatánál Magyarországon. Teljes átdolgozását a Kürt Rt. elvégezte, de jelen pillanatban az anyag nyilvánosság elé kerülésének idõpontja nem ismert.
- Ez a dokumentum az informatikai rendszerek, fõleg külsõ auditálásához nyújt használható módszertant.
- A kockázatelemzés elvégzéséhez szükséges adatok megszerzéséhez nem ad semmilyen támpontot.
- A gyakorlati megvalósításnál több kockázati mátrixot kell készíteni és ezek után vagy következtetéseket vonhatunk le a kapott eredményekbõl vagy a mátrixokban kapott eredményeket valamilyen szabály szerint még összegezzük. Erre vonatkozóan nem ad tanácsot az ajánlás.

A COBIT elõnyei és hátrányai:

- A COBIT-ot az IT Governance Institute[16] fejlesztette ki. Mivel az IT Governance Institute nem egy nemzeti hatóság, hanem egy egész világot képviselõ független szervezet, így lehetõség nyílik arra, hogy minden kontinensen elfogadják az általa létrehozott nyílt szabványt.
- A COBIT a felhasználótól jelentõs kezdeti energia-ráfordítást követel meg a szokatlan szemléletmódja miatt.

[16] IT Governance Institute-t az ISACA és az ISACF hozta létre 1998-ban.
ISACA (Information Systems Audit and Control Association) több mint száz országban mûködõ és 2300-nál több tagot számláló nemzetközileg elismert szervezet.
ISACF: Információs Rendszer Auditorok Nemzetközi Alapítványa

- Ebben az értelemben a COBIT-ot nem nevezhetjük felhasználóbarátnak, és könnyen kezelhetõ módszernek. A fejlesztõk ezen egy leírásokat tartalmazó CD-ROM mellékelésével próbálnak segíteni.
- Eddig magyar nyelvre hivatalosan teljes egészében a COBIT-ot még nem fordították le, de készül egy magyar nyelvû változat.
- A COBIT nem sok támogatást nyújt az elemzés eredményének ábrázolásához. Az utólag gyártott CD-ROM-on van néhány hasznos javaslat az elemzés táblázatos megjelenítésére.
- Léteznek szoftverek (nem magyar nyelvûek), amelyek segítik a COBIT használatát.
- A COBIT-ot ténylegesen biztonsági audithoz használják, az informatikai audittal foglalkozó cégek honlapján szinte mindig történik hivatkozás a COBIT-ra (Kürt Rt., Synergon Rt., OGYS Consulting Kft., Bull Magyarország, AAM Vezetõi Informatikai Tanácsadó Kft.,…). A COBIT kockázatelemzéshez is használható, csak nem segíti a kockázatok mennyiségi kiértékelését.
- A COBIT alkalmazásához szükséges befektetéseket elsõsorban a nagy és fejlett informatikával rendelkezõ vállalatok tudják megindokolni és megvalósítani.

A MARION eljárás elõnyei és hátrányai:

- A MARION eljárás legnagyobb pozitívuma az összefoglaló jellegében és a grafikus ábrázolásában rejlik.
- A gyengepont-elemzés érzékennyé teszi az érintetteket és segíti a következõ szakasz elemzéseit.
- A kérdések saját belátás szerinti megválaszolását az elsõ fázisban és a hosszadalmas második szakaszt említhetjük hátrányként.
- A MARION rozetta alapján, minden részletes tanulmányozás nélkül, a biztonsági felkészültség homogenitásáról azonnal képet kapunk.
- A módszer a megfelelõ tájékoztatás után könnyen alkalmazható és felhasználható.
- Nagy elõny az elektronikus kérdõívek évenkénti aktualizálása, és szervezeti sajátosságokhoz való igazításának lehetõsége.
- Gyengeségként az ismételhetõség problémáját említhetnénk, nem biztosított, hogy valaki éppen a saját eredményéhez jut vissza, ha több alkalommal végigvezeti a vizsgálatot.

Minden egyes kérdõívet elõször franciául készítenek el, majd angolra fordítják. A tapasztalat szerint az angol fordítás jó, hivatalos magyar fordítást nem említ a szakirodalom.

Az IT-Grundschutzhandbuch elõnyei és hátrányai:

- Az IT –Sicherheitshandbuch még nem, de az IT-Grundschutzhandbuch már veszély- és kockázatelemzést is tartalmaz.
- Mellõzi a hosszadalmas és gyakran haszontalan fenyegetés-scenáriók diszkusszióját.
- Az ajánlott intézkedéseknek nagy hasznuk van a gyakorlatban.
- Gyors és átfogó, közepes védelmi szintet lehet elérni a segítségével.
- Az intézkedési katalógus használata katasztrófa-megelõzésre is alkalmas.
- Az IT alapvédelem nem célorientált, a célok burkoltan, a kiválasztott intézkedések által jutnak kifejezésre.
- A mérhetõ elõnyök megfogalmazásával markánsan növelhetõ lenne a motiváció és a végrehajthatóság.

Ahhoz, hogy a felsorolt módszereket valamilyen módon össze lehessen hasonlítani, megfelelõ összehasonlítási szempontok szükségesek.

Összehasonlítási kritériumok:

Színvonal:

Nemzetközileg védett módszerek és eljárások széles szakmai elfogadottsággal. Azon módszerek, eljárások, amelyek szabványosításra kerültek.

Függetlenség:

A módszer alapvetõen független, ez azt jelenti, hogy gyártó vagy tanácsadó bevonása nélkül is alkalmazhatóvá válik.

Minõsíthetõség:

A módszer megengedi harmadik fél bevonásával a felhasználó minõsítését, objektív eljárás keretében.

Realizálhatóság:

A módszer gyakorlat- és intézkedésorientált. Intézkedései közvetlenül konkrét helyzetbe átvihetõk, transzformálhatók.

Alkalmazhatóság:

A módszer minden szervezetre, esetleg eszközre felhasználható. Megfelelõ ráfordítással speciális szükségletekhez is alakítható.

Értékelési terjedelem:

A módszer egy teljes témakör feldolgozását biztosítja. A módszerek és eljárások a feldolgozás mélységében és szélességében elõre skálázhatók.

Eredmény-ábrázolás:

A módszer támogatja a kitûzött céloknak megfelelõ eredmények áttekinthetõ és gyorsan érthetõ ábrázolását.

Gazdaságosság:

A módszer megfelelõ idõn belül vezet eredményhez. A ráfordítás-haszon arány átlátható és végrehajtható.

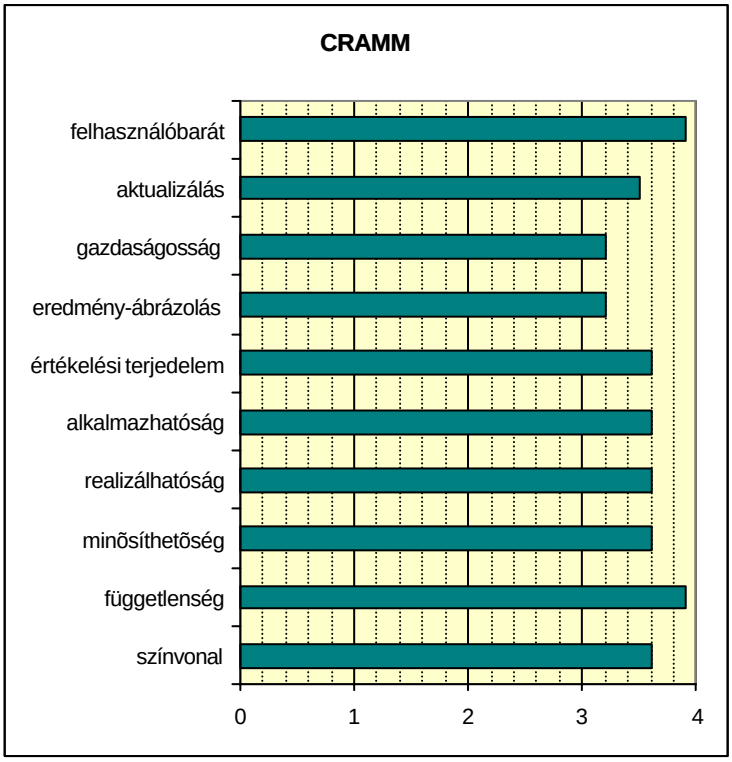
Aktualizálás:

A tartalom rendszeresen aktualizált ill. bõvített. Minden új változtatás a saját elõdjével kompatíbilis.

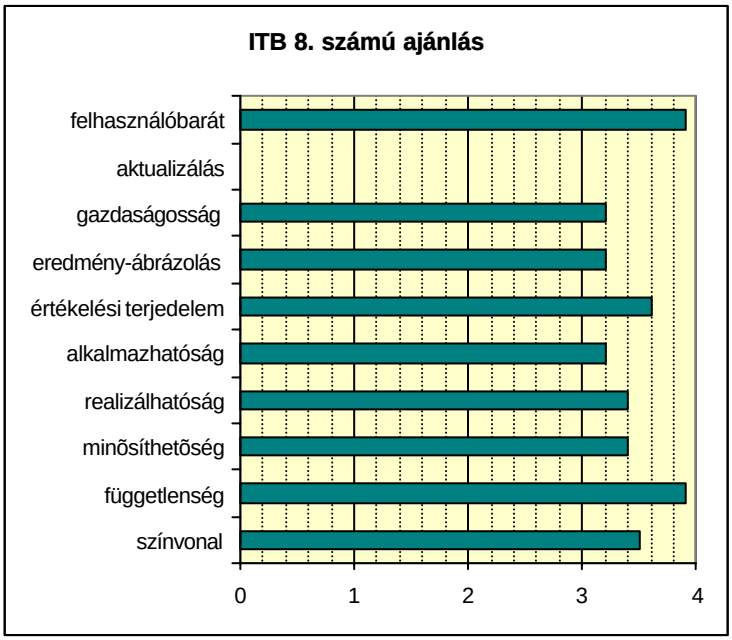
Felhasználóbarát:

A módszer nem nagy tanulási ráfordítással használható, segíti a felhasználót a munka elvégzésében.

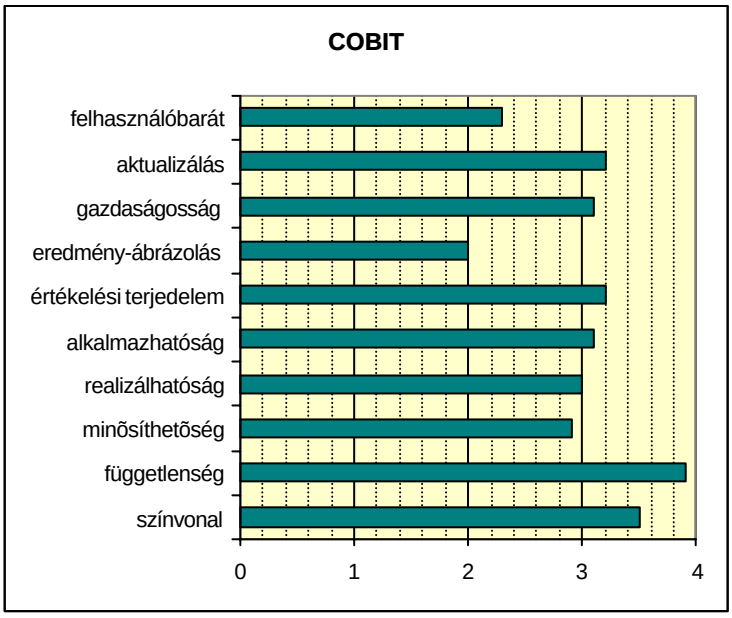
A CRAMM, az ITB ajánlások, a COBIT, a MARION, az IT- Grundschutzhandbuch elõzõ szempontok szerinti összehasonlításához, a szakirodalom tanulmányozásán és a kockázatelemzési tapasztalataimon kívül, felhasználtam az ISACA honlapján a témában megjelent publikációkat, másrészt olyan cégek informatikai audittal foglalkozó szakembereinek a véleményét vettem figyelembe, akik a témában elismertek.



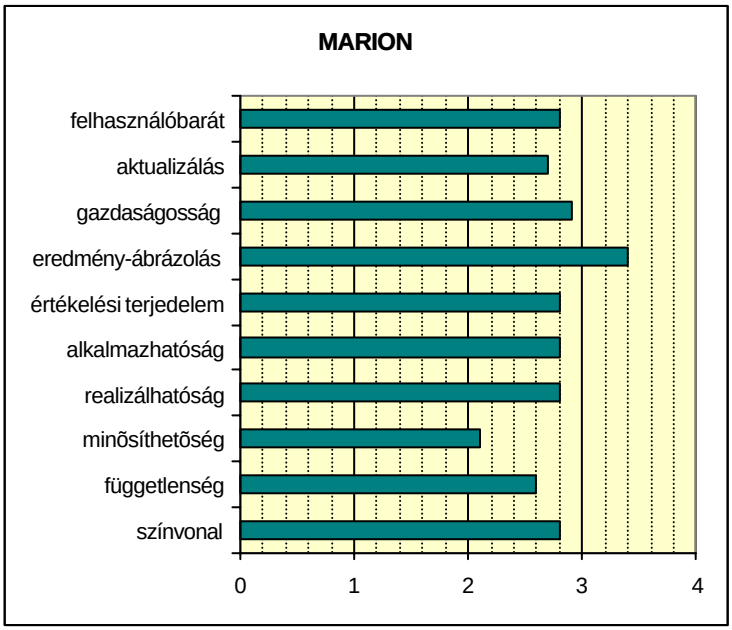
A grafikonról a függetlenség, a felhasználó munkájának megkönnyítésére vonatkozó törekvés tükrözõdik és negatívumként jelentkezik az eredményábrázolás és a gazdaságosság.



Ugyanúgy, mint a CRAMM-nél a függetlenség és a felhasználó támogatottsága a legjobb tulajdonság, feltûnik a rendszeres aktualizálás hiánya.



A grafikonról is leolvasható, hogy az eljárás készítõi nagy hangsúlyt helyeztek az ún. függetlenségre és a színvonalra. A felhasználói támogatottság és az eredmények grafikus ábrázolása a COBIT gyenge oldala.



A MARION-nál az eredmények nagyon kiegyensúlyozottak, a grafikus ábrázolása kiemelkedik, ez a legnagyobb pozitívuma a módszernek. A minõsíthetõséget és értékelhetõséget nem támogatja a Franciaországban nagymértékben elterjedt módszer.

Ennél a módszernél feltûnik a folyamatos aktualizálás és a szerkesztõktõl való függetlenség. Nem meggyõzõ a felhasználók támogatása és az eredmények ábrázolása.

2.3. Veszélyelemzõ módszerek

A veszély és a kockázat fogalmakat nem minden nyelv különbözteti meg, a kockázat mai értelmezése a 17. 18. században az angol nyelvben a biztosításokkal kapcsolatban alakult ki. A szakirodalomban is elõfordul, hogy az itt felsorolt veszélyelemzõ módszereket kockázatelemzõ módszereknek nevezik. Ebben a fejezetben a leggyakoribb veszélyelemzõ módszereket vizsgálom és hasonlítom össze.

2.3.1. Hibafa elemzés

A hibafa elemzés (**F**ault **T**ree **A**nalysis - FTA) deduktív, explikációs[17] eljárás az okozat felõl halad az okok felé. Ez a megoldás egy fa típusú irányított gráf felépítésén alapszik, amely szerint valamely nem kívánatos eseményt, amit közvetlenül nem áll módunkban elhárítani, illetve megelõzni, logikai módszerekkel egyszerûbbekre, hatáskörünkben állókra vezetjük vissza. A hatások fegyelembevételénél logikai (Boole) operátorokat használunk. A hibafában csak azok az események szerepelnek, amelyek veszélyeztetõ hatásúak, így az FTA-struktúra nem túl bonyolult és követhetõ. A hibafa csúcsán a nem kívánt esemény szerepel, amelyhez logikai mûveletek (ÉS, VAGY, NEM, …) csatlakoznak.

A hibafa elemzés lépései:

- A biztonságot meghatározó részrendszerek definiálása és egymástól való elhatárolása.
- A rendszer feladatainak és követelményeinek vizsgálata.
- A nem kívánt események számbavétele, meghatározása.
- A hibák közötti logikai összefüggések feltárása és ábrázolása a hibafán.
- Az értékelés, a számítások elvégzése.

A hibafa minõségi kiértékelése:

Ha mérõszámok nélkül akarunk következtetéseket levonni, akkor a minimális kritikus láncokat kell megkeresni. A minimális lánc egy hibakombináció, ami a lehetõ legkisebb számú meghibásodás mellett egy nem kívánt esemény bekövetkezését okozza, ez a hibafa leggyengébb ága és itt szükséges a változtatás.

A hibafa mennyiségi kiértékelése:

A rendszerelemekre vonatkozó megbízhatósági mérõszámokból kiindulva kiszámítható a fõesemény bekövetkezési valószínûsége. A kiinduló adatokat szakkönyvekbõl, táblázatokból, gyakorlati tapasztalatból vagy különbözõ tesztek, vizsgálatok alapján lehet meghatározni.

Az ÉS kapuk kimenti valószí nûségének kiszámí tása: $q = \prod_{i=1}^{n} q_i$

A VAGY kapuk kimeneti valószí nûsége: $q = \sum_{i=1}^{n} q_i$ (egymást kizáró események esetén)

$$q = 1 - \prod_{i=1}^{n} (1 - q_i) \quad \text{(általános esetben)}$$

A számszerû eredmény (egy valószínûségi érték) megmutatja, hogy a rendszer megfelel-e az elvárásoknak. A rendszer gyenge pontjairól a minimális metszetek halmazán keresztül lehet információt szerezni. Minimális metszet az elemi események azon halmaza, mely elemi események együttes bekövetkezésekor a fõesemény

[17] a latin explicare = kifejteni, explicitté tenni alapján

bekövetkezik, de amelyek közül bármelyik esemény be nem következésekor a fõesemény sem következik be. A minimális metszetekhez hozzárendelik a bennük szereplõ elemi események bekövetkezési valószínûségének szorzatát. A minimális metszeteket érték szerint sorba rendezve megállapítható, hogy elsõsorban melyik elemi események felelõsek a csúcsesemény bekövetkezéséért. A minimális metszetek további elemzésével megállapítható az is, hogy minimálisan hány hiba szükséges a fõesemény bekövetkezéséhez.

A következõkben néhány fogalmat kell meghatározni.

Hibaállapotok:

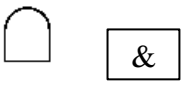
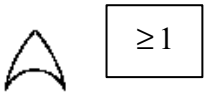
Az alkotóelemek meghibásodásai három osztályba sorolhatók; elsõdleges hiba, másodlagos hiba, kezelési hiba.

Elsõdleges hibának nevezzük azt a meghibásodást, amely elõírt mûködési körülmények között áll elõ, az ok az alkotóelem kialakításában vagy az anyag tulajdonságaiban lehet.

Másodlagos hibának nevezzük azt a meghibásodást, amely a nem megengedett külsõ behatások következtében áll elõ (pl. környezeti feltételek, alkalmazási körülmények)

Kezelési hibák a nem megfelelõ használat, kezelés miatt alakulhatnak ki.

A hibafa képjelei az IEC 1025 szabvány és más elfogadott megállapodások szerint:

KÉPJEL	FUNKCIÓ	JELENTÉS
	Az esemény leírása	Ebben a képjelben adható meg az esemény megnevezése, jellemzése, kódja vagy a bekövetkezési gyakoriság.
	Alapesemény	Tovább már nem bontható esemény, hiba
	ÉS	ÉS kapu, az esemény csak akkor következik be, ha mindkét bemenõ esemény egyszerre bekövetkezik.
	VAGY	VAGY kapu, az esemény akkor következik be, ha legalább egy bemenõ esemény bekövetkezik.
	Átvitel	Átvezetés, a hibafában máshol elõforduló esemény.
	Külsõ esemény	Külsõ, szokásos esemény, nem hiba
	Másodlagos hiba	Nem kell tovább vizsgálni

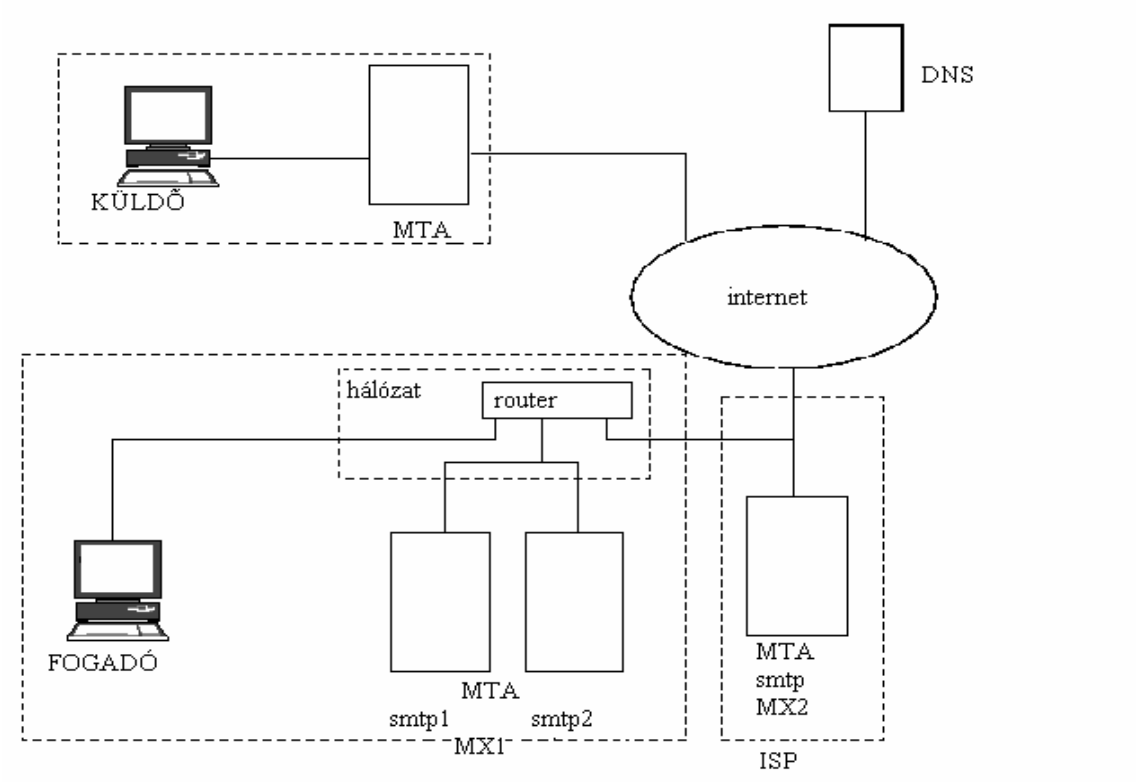
2.3. ábra. A hibafák képjelei

Példa a hibafára[18]*:*

Alapesemény: az érkezõ levél elveszett.

Követelmény: világosan és egyértelmûen meg kell fogalmazni, hogy mi történt, a hibafa választ ad arra, hogy hogyan történt.

Rendszer-meghatározás:



2.4. ábra. Egyszerû példa hibafa elemzésre; rendszer-meghatározás

MTA (mail transfer agent=levéltovábbító egység):

MX1: a helyi hálózat fogadja a levelet? *MX2: az ISP MTA-ja fogadja a levelet?*

ISP (Internet Service Provider= Internet Szolgáltató), minden internet forgalom, amely egy adott géphez érkezik, vagy onnan indul, az internet szolgáltatójának ISP rendszerén halad keresztül. Az ISP kapcsolja az adott gépet az internethez.

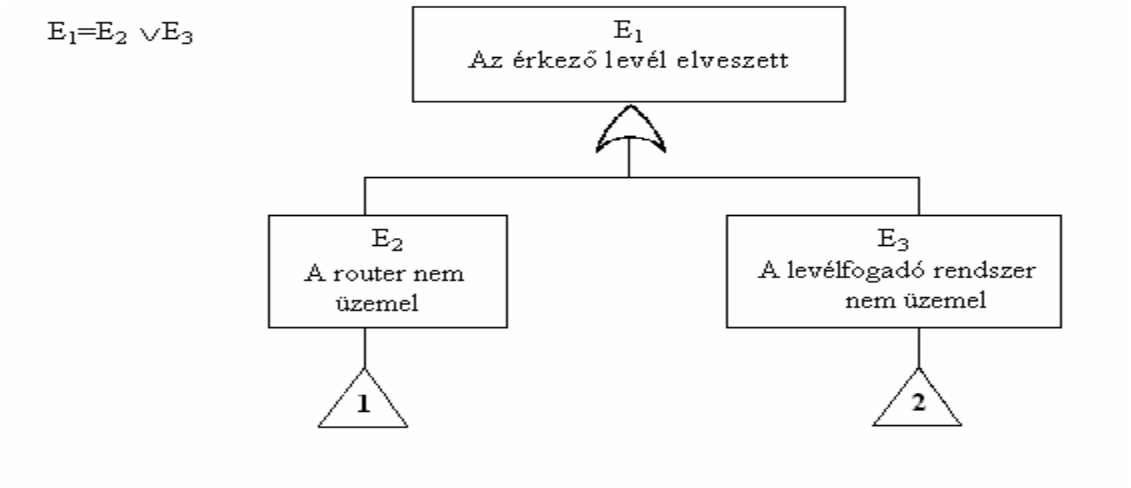
Smtp (Simple Mail Transfer Protocol): SMTP Internet szabvány az elektronikus levelek továbbítására

Router: az alhálózatokat összekötõ berendezés protokolokkal

DNS: név-felismerés

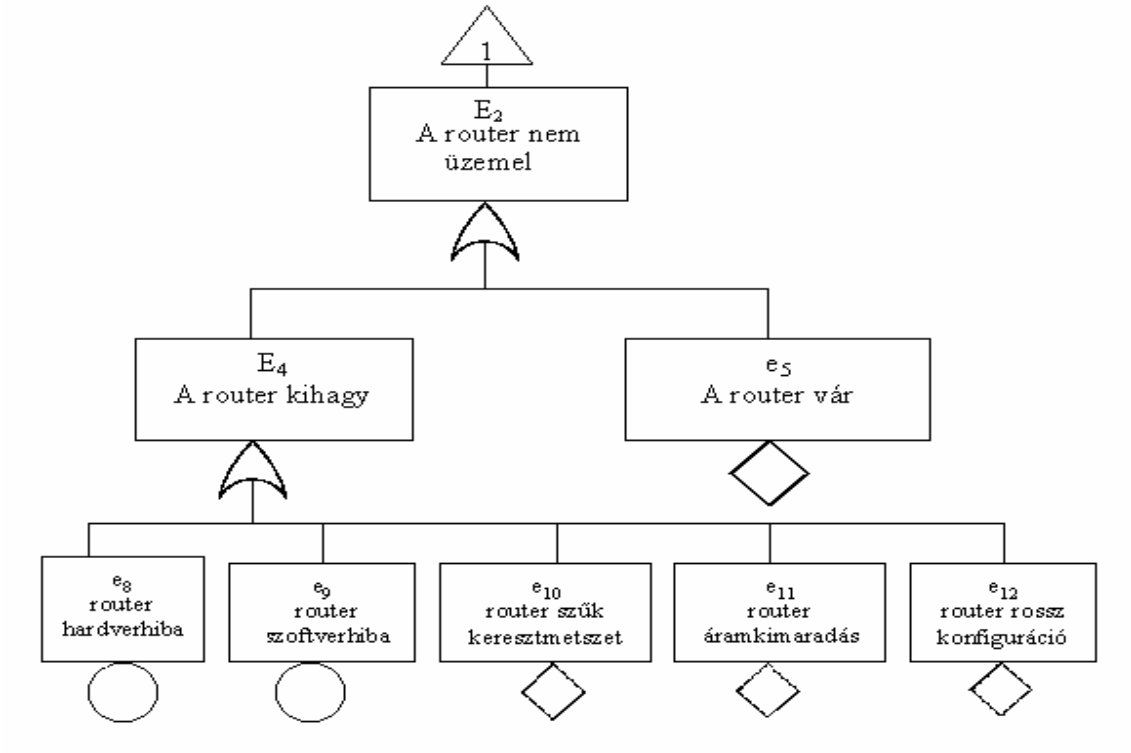
[18] Forrás: Dienste: Zuverlässigkeit, Verfügbarkeit und Ausfallrisiken. http://archiv.tu-chemnitz.de/pub/2002/01

1. hibafa:



2.5. ábra. Egyszerû példa hibafa elemzésre; 1. hibafa

2.hibafa:



2.6. ábra. Egyszerû példa hibafa elemzésre; 2. hibafa

$E_2=E_4 \vee e_5$

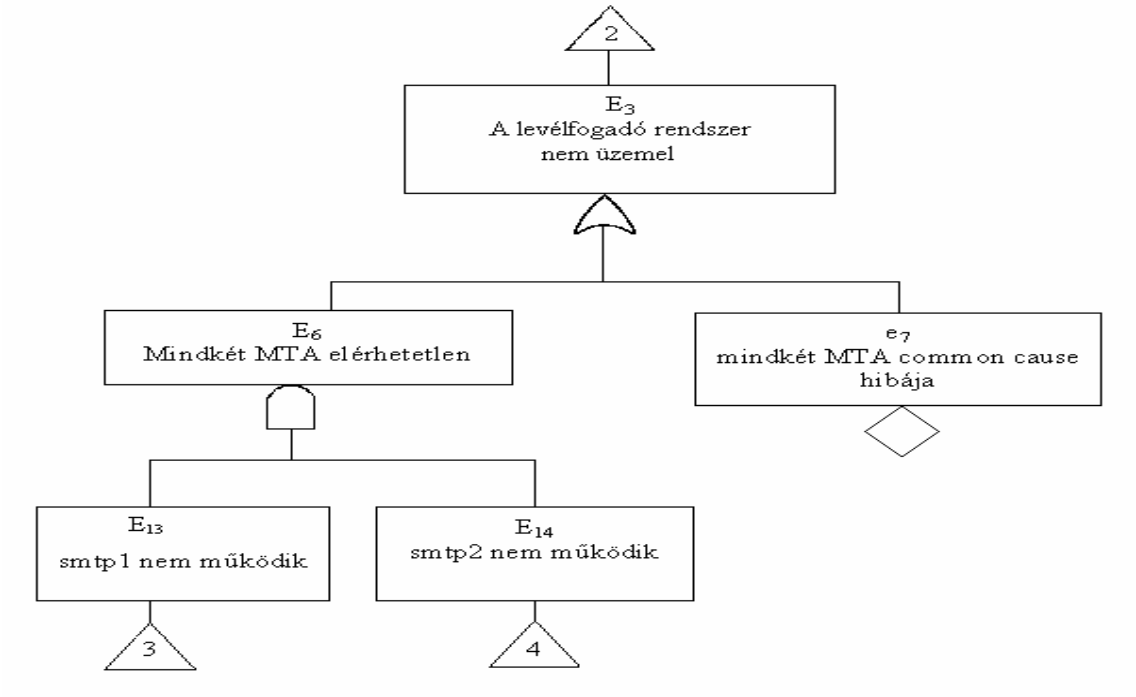
$E_4=e_8 \vee e_9 \vee e_{10} \vee e_{11} \vee e_{12}$

Megjegyzés:

„E”: tovább vizsgálandó esemény

„e”: tovább nem bontható vagy nem vizsgálandó esemény

3.hibafa:

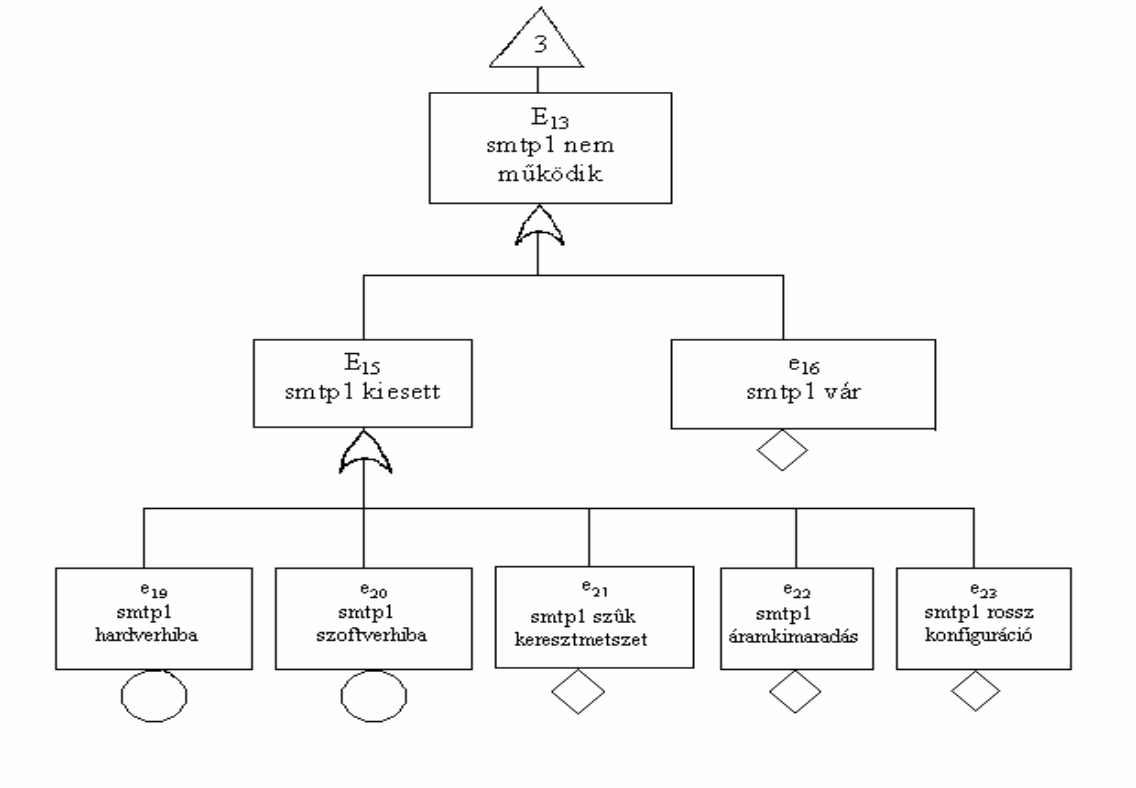


2.7. ábra. Egyszerû példa hibafa elemzésre; 3. hibafa

$E_3=E_6 \vee e_7$; $E_6=E_{13} \wedge E_{14}$

Megjegyzés: e_7 : mindkét MTA közös okra visszavezethetõ hibája

4. hibafa:

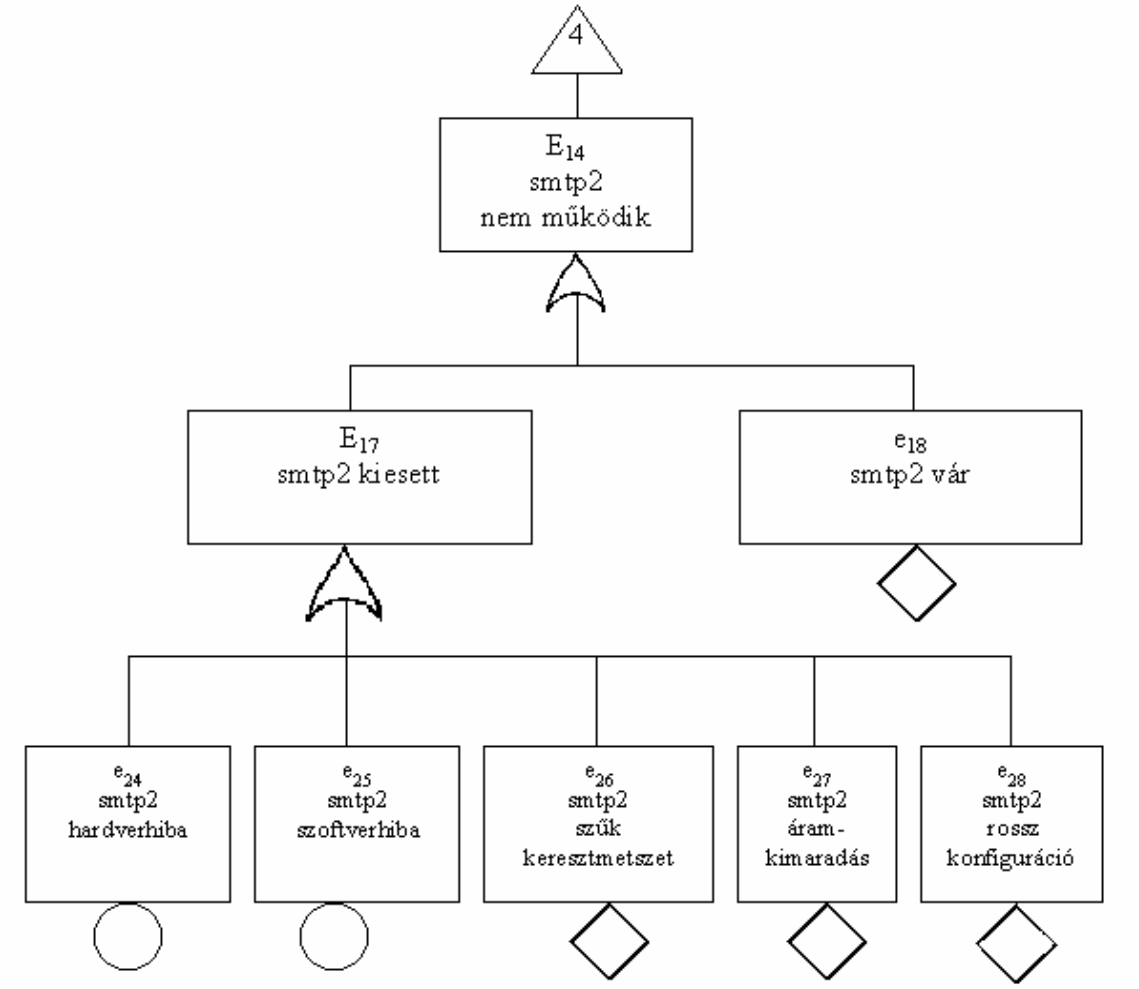


2.8. ábra. Egyszerû példa hibafa elemzésre; 4. hibafa

$E_{13}=E_{15} \vee e_{16}$

$E_{15}=e_{19} \vee e_{20} \vee e_{21} \vee e_{22} \vee e_{23}$

5. hibafa:



2.9. ábra. Egyszerû példa hibafa elemzésre; 5. hibafa

$E_{14}=E_{17} \vee e_{18}$

$E_{17}=e_{24} \vee e_{25} \vee e_{26} \vee e_{27} \vee e_{28}$

A minimális metszethalmazok meghatározása:

A minimális metszetek a rendszer gyenge pontjairól adnak felvilágosítást.

1. Elõállítandó a hibafa Boole-algebrai megfelelõje.

$E_1=E_2 \vee E_3=(E_4 \vee e_5) \vee (E_6 \vee e_7)=(e_8 \vee e_9 \vee e_{10} \vee e_{11} \vee e_{12} \vee e_5) \vee ((E_{13} \wedge E_{14}) \vee e_7)=$

$=(e_8 \vee e_9 \vee e_{10} \vee e_{11} \vee e_{12} \vee e_5) \vee (((E_{15} \vee e_{16}) \wedge (E_{17} \vee e_{18})) \vee e_7)=$

$=(e_8 \vee e_9 \vee e_{10} \vee e_{11} \vee e_{12} \vee e_5) \vee ((((e_{19} \vee e_{20} \vee e_{21} \vee e_{22} \vee e_{23}) \vee e_{16})$

$\wedge ((e_{24} \vee e_{25} \vee e_{26} \vee e_{27} \vee e_{28}) \vee e_{18})) \vee e_7)=$

$=(e_5 \vee e_7 \vee e_8 \vee e_9 \vee e_{10} \vee e_{11} \vee e_{12}) \vee ((e_{16} \vee e_{19} \vee e_{20} \vee e_{21} \vee e_{22} \vee e_{23}) \wedge$

$(e_{18} \vee e_{24} \vee e_{25} \vee e_{26} \vee e_{27} \vee e_{28}))=$

$$=e_5 \vee e_7 \vee e_8 \vee e_9 \vee e_{10} \vee e_{11} \vee e_{12} \vee$$
$$e_{16}e_{18} \vee e_{16}e_{24} \vee e_{16}e_{25} \vee e_{16}e_{26} \vee e_{16}e_{27} \vee e_{16}e_{28} \vee$$
$$e_{19}e_{18} \vee e_{19}e_{24} \vee e_{19}e_{25} \vee e_{19}e_{26} \vee e_{19}e_{27} \vee e_{19}e_{28} \vee$$
$$e_{20}e_{18} \vee e_{20}e_{24} \vee e_{20}e_{25} \vee e_{20}e_{26} \vee e_{20}e_{27} \vee e_{20}e_{28} \vee$$
$$e_{21}e_{18} \vee e_{21}e_{24} \vee e_{21}e_{25} \vee e_{21}e_{26} \vee e_{21}e_{27} \vee e_{21}e_{28} \vee$$
$$e_{22}e_{18} \vee e_{22}e_{24} \vee e_{22}e_{25} \vee e_{22}e_{26} \vee e_{22}e_{27} \vee e_{22}e_{28} \vee$$
$$e_{23}e_{18} \vee e_{23}e_{24} \vee e_{23}e_{25} \vee e_{23}e_{26} \vee e_{23}e_{27} \vee e_{23}e_{28}$$

Ez a kifejezés a modell metszethalmazait tartalmazza, de nem a minimális metszethalmazokat.

2. A minimális metszethalmazok meghatározásához ezeket a metszeteket redukálni kell.

   Az adott példában elképzelhetõ, feltételezhetõ, hogy közös áramforrása van mindegyik eszköznek, így e_{11}, e_{22}, e_{27} azonosak.

   $$E_1=e_5 \vee e_7 \vee e_8 \vee e_9 \vee e_{10} \vee e_{11} \vee e_{12} \vee$$
   $$e_{16}e_{18} \vee e_{16}e_{24} \vee e_{16}e_{25} \vee e_{16}e_{26} \vee e_{16}e_{28} \vee$$
   $$e_{19}e_{18} \vee e_{19}e_{24} \vee e_{19}e_{25} \vee e_{19}e_{26} \vee e_{19}e_{28} \vee$$
   $$e_{20}e_{18} \vee e_{20}e_{24} \vee e_{20}e_{25} \vee e_{20}e_{26} \vee e_{20}e_{28} \vee$$
   $$e_{21}e_{18} \vee e_{21}e_{24} \vee e_{21}e_{25} \vee e_{21}e_{26} \vee e_{21}e_{28} \vee$$
   $$e_{23}e_{18} \vee e_{23}e_{24} \vee e_{23}e_{25} \vee e_{23}e_{26} \vee e_{23}e_{28}$$

Minden hibafához véges számú minimális metszethalmaz határozható meg.

A hibafa elemzés pozitívumai:

- Lehetõvé teszi a fõeseményhez vezetõ összes hiba és hibakombináció, valamint ezek okainak azonosítását.
- Segítségével kimutatható a különösen kritikus események és esemény-láncolatok.
- A hibafa ágain végighaladva megbízhatósági számértékeket határozhatunk meg.
- A meghibásodási mechanizmusok tisztán és áttekinthetõen dokumentálhatók.
- Az FTA segítségével igen egyszerû a különbözõ biztonsági intézkedések kihatásainak kutatása.

2.3.2. Eseményfa elemzés

Az eseményfa elemzés (**E**vent **T**ree **A**nalysis – ETA) során olyan eseményeket tételeznek fel, amelyek hatással lehetnek a rendszer mûködésére, az analízis során ezeknek a hatását követik végig. Nemcsak a lehetséges hibaeseményeket, hanem a normál módon betervezetteket is figyelik, mivel az ilyenekbõl is következhet biztonsági probléma. Az eseményfa egy fa típusú irányított gráf, amelynek gyökere a kiindulási esemény, ezt követõen pedig annak hatásai szerint ágazik szét a különbözõ szinteken. Ha egy végsõ kimenetel veszélyt jelent, akkor intézkedéseket kell hozni a rendszer

mûködésével kapcsolatban. Az eseményfa elemzésnek minõségi és mennyiségi kiértékelése is lehet, a mennyiségi kiértékelésnél az eseményfában feltüntetett valószínûségek feltételes értékek.

Az eseményfa megszerkesztésének lépései: [6]

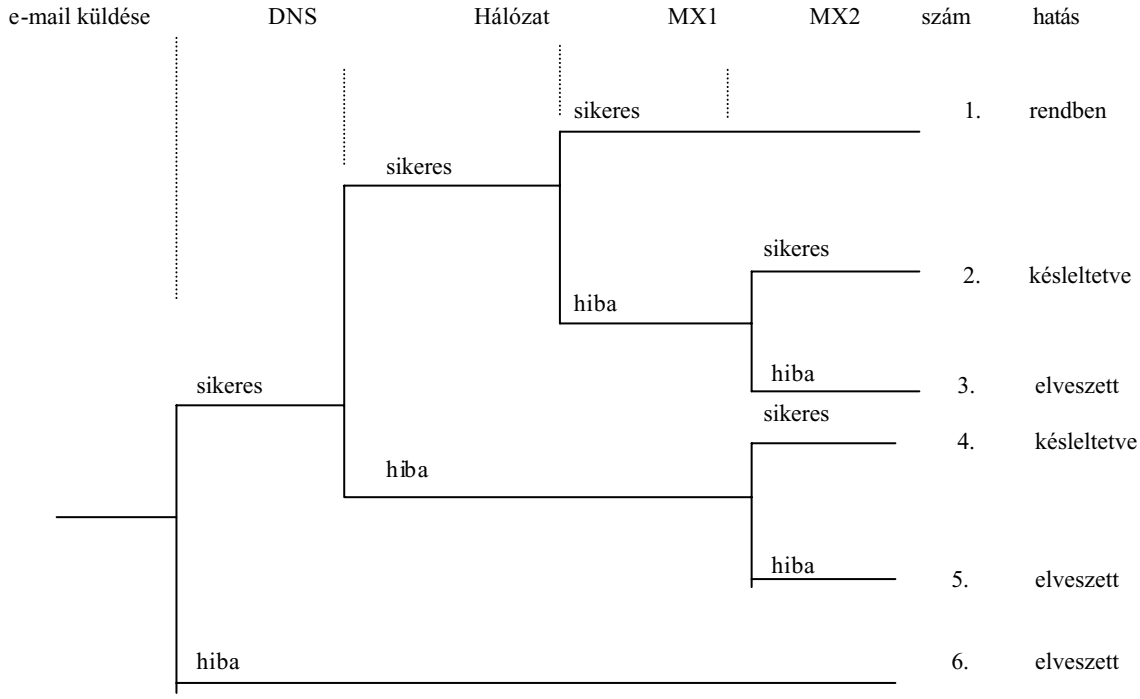
- a kezdeti esemény definiálása,
- a kockázat definiálása,
- azoknak az eljárásoknak a definiálása, amelyek során felléphet a kockázat

Egy konkrét példánál, ami egy e-mail elküldése, ez a következõt jelenti:

- definiáljuk a kezdeti eseményt; egy e-mail küldése adott címre
- a kockázat; a levél elveszik,
- eljárások;

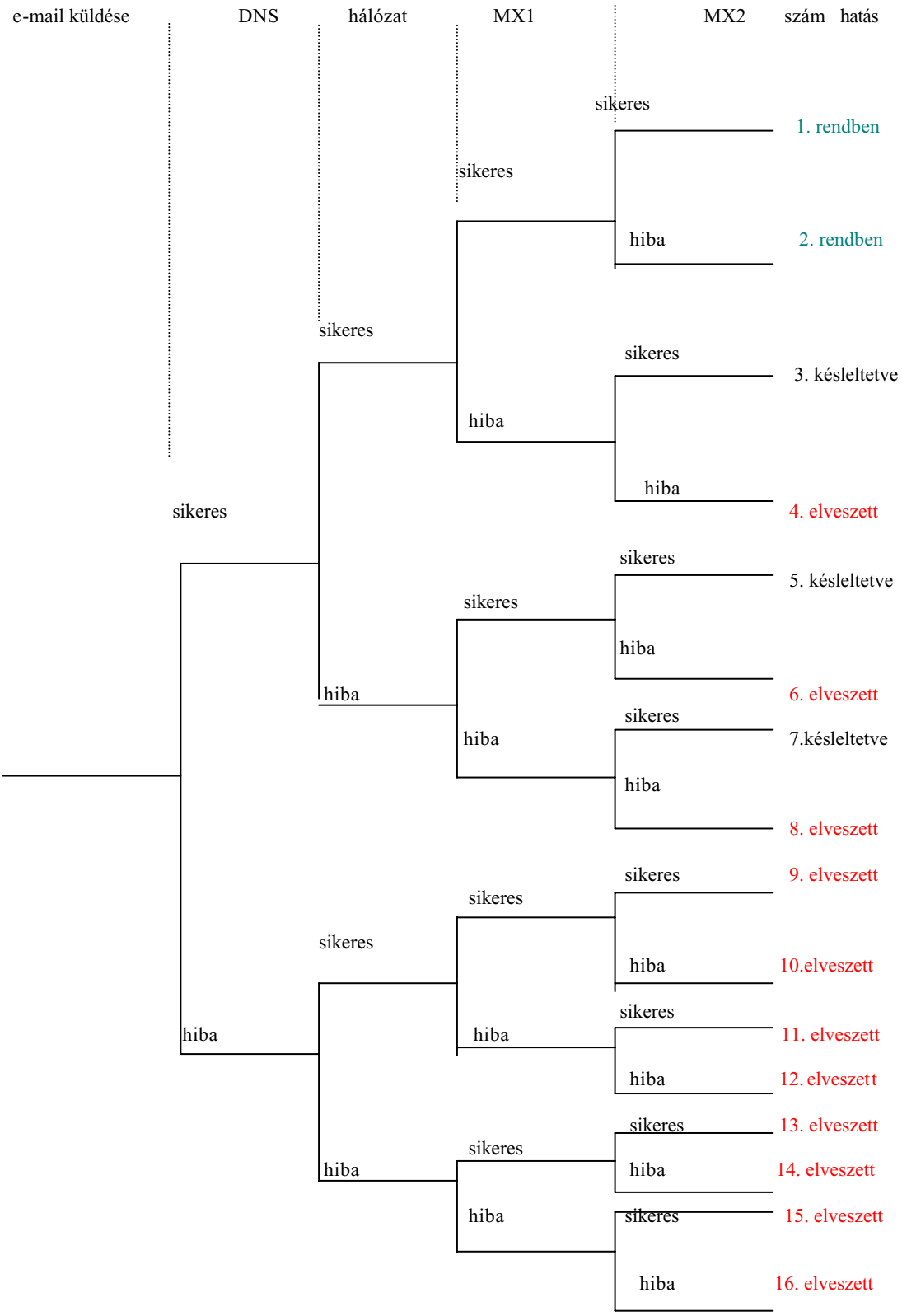
DNS: név-felismerés (a szükséges név felismerhetõ?)
Hálózat: elérhetõ-e a helyi MTA?
MX1: a helyi MTA fogadja a levelet?
MX2: az ISP MTA-ja fogadja a levelet?

Az eseményfa egyszerûsített formája:



2.10. ábra. Egyszerû példa eseményfa elemzésre; az eseményfa egyszerûsített formája

A teljes eseményfa:



2.11. ábra. Egyszerû példa eseményfa elemzésre; teljes eseményfa

A valószínûségek meghatározása:

Minden egyes elágazáshoz valószínûségeket rendelünk, amelyek különbözõ tesztek elvégzésébõl kapott vagy múltbeli tapasztalatok alapján megállapított értékek lehetnek.

- P_{DNS}: A DNS megbízhatósága
- $P_{Hálózat}$: A hálózat megbízhatósága
- P_{MX1}: Az MX1 megbízhatósága
- P_{MX2}: Az MX2 megbízhatósága
- $P_{e\text{-}mail}$: Annak a valószínûsége, hogy a vizsgált idõintervallumban egy e-mail megérkezik

- Az azonnali levélkézbesítés valószínûsége:

$$P_{rendben} = P_1 = P_{e\text{-}mail} * P_{DNS} * P_{Hálózat} * P_{MX1} * (P_{MX2} + (1 - P_{MX2})) =$$
$$= P_{e\text{-}mail} * P_{DNS} * P_{Hálózat} * P_{MX1}$$

- A késleltetett levélkézbesítés valószínûsége:

$$P_{késleltetve} = P_2 + P_4$$
$$P_2 = P_{e\text{-}mail} * P_{DNS} * P_{Hálózat} * (1 - P_{MX1}) * P_{MX2}$$
$$P_4 = P_{e\text{-}mail} * P_{DNS} * (1 - P_{Hálózat}) * P_{MX2}$$

(az eseményfa *egyszerûsített* formája alapján ez az összefüggés jól látható)

$$P_{késleltetve} = P_2 + P_4 = P_{e\text{-}mail} * P_{DNS} * P_{Hálózat} * (1 - P_{MX1}) * P_{MX2} +$$
$$+ P_{e\text{-}mail} * P_{DNS} * (1 - P_{Hálózat}) * P_{MX2} =$$
$$= P_{e\text{-}mail} * P_{DNS} * P_{MX2} (P_{Hálózat} * (1 - P_{MX1}) + 1 - P_{Hálózat}) =$$
$$= P_{e\text{-}mail} * P_{DNS} * P_{MX2} * (1 - P_{Hálózat} * P_{MX1})$$

- A kockázat, a levél elvesztésének valószínûsége:

$$P_{elveszett} = P_3 + P_5 + P_6 = 1 - (P_1 + P_2 + P_4) = 1 - P_{rendben} - P_{késleltetve}$$

Ez a fa-szerkezet sok eseménynél már áttekinthetetlen a sok elágazás miatt, ezért alkalmazását hibafa elemzéssel kombinálják.

Végül a két elemzést összefoglalva: A *hibafa* létrehozásakor általában több szint jön létre, a legfelsõ szinten a csúcsesemény, ami a hibának a vizsgált rendszerre gyakorolt hatását jelenti, a következõ szinten a hiba kiváltásához közvetlenül szükséges valamennyi hibalehetõség, ezek mindegyikébõl újabb elágazás indul ki, amelyek közül valamelyik elvezet a kiváltó okhoz, az alapeseményhez.

A hibafa létrehozásának az elõnyei: Az a rendszer, amelynek a mûködésére egy hibafa áll rendelkezésre jól áttekinthetõ, érthetõ. A hibafa kidolgozása során rendelkezésünkre áll a kiváltó okok listája, amelynek a segítségével javítani lehet a rendszer mûködését anélkül, hogy valószínûséget vagy gyakoriságot számoltunk volna.

A hatáselemzésekhez jól használható az *eseményfa.* Az eseményfa kiindulópontja a kezdeti esemény és vizsgáljuk a további események bekövetkezésének lehetõségeit, az eseményláncokat. Elõfordulhat, hogy az eseményfa kezdeti eseménye a hibafa csúcseseménye.

2.3.3. Hibamódok és hatásuk elemzése

A hibamódok és hatásuk elemzésénél (**F**ailure **M**ode and **E**ffects **A**nalysis – FMEA) komponens-hibákat tételeznek fel, célja a lehetséges rendszer meghibásodások felfedése. Végigkövetik a hiba hatását a teljes mûködésen keresztül. Az elemzést hardver elemekre vagy funkciókra vonatkoztatva végzik. Az elemzés során figyelembe veszik a rendszer valamennyi elemének, funkciójának valamennyi lehetséges hibamódját.

Az FMEA vizsgálat lépései;

- a vizsgálat alapjainak definiálása (mûködési fázisok, mûködési környezet, a mûködés célja stb.),
- az analízisvégzés szintjének definiálása (a rendszer egy-egy részterülete, vagy az egész rendszer),
- az egyes vizsgálandó egységek, alegységek definiálása (alrendszer, modul, funkció, komponens),
- a vizsgált komponensek lehetséges meghibásodási módjainak összegyûjtése, hibakatalógus készítése.
- minden egyes komponens lehetséges meghibásodási módjai következményeinek feltárása,
- a következmények osztályozása a rendszermûködésre gyakorolt hatásuk alapján,
- az egyes meghibásodási módok detektálhatóságának vizsgálata,
- szükség esetén a kompenzációs módok vagy tervváltoztatások vizsgálata a veszélyesnek ítélt meghibásodások hatásainak elkerülésére. [7]

A módszer minden lehetséges hibát figyelembe vesz, különösen alkalmas az egyszeres hibák meghatározására. Az életciklus különbözõ fázisaiban is alkalmazható; a korai fázisában, funkciókra, a késõbbi fázisokban hardver elemekre alkalmazva, az egyes szinteken az elemzés finomítására is használható. A módszer negatívumai: nem veszi figyelembe a többszörös hibákat, ezzel szemben olyanokat is figyelembe vesz, amelyek nem okoznak igazi veszélyeztetést, így a nagy rendszerekben rendkívül ráfordítás-igényes, ezért sok esetben csak a fejlesztési folyamat végsõ fázisaiban, és ott is a kritikus területek vizsgálatára alkalmazzák.

Összehasonlítva az FMEA és a FTA –t; az FMEA induktív eljárás, értékeli az egyes elemek meghibásodásának gyakoriságát és a következményeket, minden elemre minden meghibásodást figyelembe vesz. Az FMEA elemzés formálisan elvezethet a hiba okának feltárásához, de erre nem igazán alkalmas. Az FTA deduktív eljárás, a hibához vezetõ összes kritikus utat feltárja, a hiba okát keresi, a gyakorlatban jól alkalmazható a különbözõ biztonsági intézkedések hatásának vizsgálatához és a baleseti okok meghatározásához is.

2.3.4.Veszély és mûködõképesség elemzés

A veszély és mûködõképesség elemzés (**Haz**ardous and **Op**erability Reviews - HAZOP) alapvetõ veszélyazonosítási technika, az FMEA egyik formája, megvizsgálja a rendszer minden egyes részét, a rendeltetésszerû mûködéstõl eltérõ lehetséges állapotokat, meghatározza a változások okait és következményeit. Különösen a paraméterváltozások és az elõírt tartományokból való kilépések biztonságra gyakorolt hatásának vizsgálatára alkalmas. Munka- és idõigényes, felkészült elemzõknek és teameknek ajánlott.

2.3.5. Hibamód, -hatás és kritikusság elemzés

A hibamód, -hatás és kritikusság elemzés (**F**ailure **M**odes **E**ffects and **C**riticality **A**nalysis - FMECA) az FMEA olyan kiterjesztése, amely figyelembe veszi az elemek meghibásodásainak fontosságát, az egyes hibák következményeit, fellépésének gyakoriságát, valószínûségét, Meghatározza a rendszer azon részeit, amelyekben a hibák a legkritikusabbak.

2.3.6. Veszélyelemzés az informatikai rendszer teljes életciklusában

A fejezetben arra a kérdésre keresem a választ, hogy a veszélyelemzési eljárások hogyan kísérik végig az informatikai rendszereket a teljes életciklusukban, mikor alkalmazhatók, mikor elengedhetetlenül fontos az alkalmazásuk.

PHI (Preliminary Hazard Identification= elõzetes veszélyazonosítás):

Az életciklus legkorábbi fázisában, a koncepció kialakításánál azonosítják a veszélyforrásokat, a megfelelõ intézkedések meghozatala érdekében. A veszélyazonosítást minden részrendszerre elvégzik a mûködési körülményekre, a hibákra vonatkozóan. Erre az eljárásra a HAZOP módszer alkalmazható.

A PHI eredményeit az elõzetes veszélyeztetési listában rögzítik **(Preliminary hazard list**) Ha lényeges veszélyeztetést találtak, akkor ez a lista szolgál a késõbbi veszélyelemzés alapjául. Biztonságkritikus rendszereknél az azonosított veszélyeztetéseket bejegyzik a **biztonsági naplóba.** A naplóban folyamatosan rögzítik a rendszerrel kapcsolatos biztonsági kérdéseket is. Ha nem találtak lényeges veszélyeztetést, akkor további elemzés nem szükséges, ha rendszer nem biztonságkritikus, akkor a lista annak bizonyítéka, hogy a veszélyeztetések azonosítása megtörtént.

PHA (Preliminary hazard analysis= elõzetes veszélyelemzés):

A PHA induktív módszer, a PHI során azonosított veszélyeztetések részletes elemzése valamilyen szisztematikus eljárással. A biztonsági követelményeket meghatározó fázis megalapozója, segíti a viszonylag korai döntést, a rendszer-architektúrát és az alkalmazandó technikákat illetõen, támogatja a késõbbi veszély- és biztonsági elemzési tevékenységeket.

Az elõzetes veszélyelemzés egy példáját szemlélteti a népesség-nyilvántartás információrendszerének továbbfejlesztése elõtt elvégzett analízis. [8]

Preliminary hazard analysis report (elõzetes veszélyelemzés jelentés):

Tartalmazza az elõzetes veszélyelemzés és a biztonsági vizsgálat eredményeinek leírását. Lényeges információkat adhat a rendszerrõl és a vele kapcsolatos veszélyeztetésekrõl, mint például a rendszer és környezetének rövid leírása, a rendszer funkcióinak és biztonsági jellemzõinek áttekintése, a rendszer biztonsági célkitûzései, a kockázat és az integritási szint megítélése, a meghibásodási ráta és a biztonsági szint megcélzott értéke, az elemzésben felhasznált adatok forrása, a felhasznált dokumentációk bibliográfiája.

Safety review (biztonsági vizsgálat):

A fejlesztési folyamat során többször történhet biztonsági felülvizsgálat. Az elsõ ilyen vizsgálat általában a PHA fázist követi, ha a rendszer a PHA és az ezt követõ biztonsági felülvizsgálatok alapján kevésbé tûnik kritikusnak, akkor további részletesebb veszélyelemzés nem szükséges, illetve gazdaságilag nem indokolható. A felülvizsgálatok valamennyi biztonsági szempontra kiterjednek. Az eredményeket a biztonsági naplóban (**safety log**) rögzítik.

Safety plan (biztonsági terv):

A közepesen és a nagyobb mértékben kritikus rendszerek számára részletes biztonsági tervet készítenek, és a projekt folyamán aktualizálják, hogy milyen módon érik el a kívánt biztonságot. Ez a terv tartalmazza a követendõ szabványokat, irányelveket, és azt hogy hogyan teljesítik ezeknek az elõírásait.

SHA (Safety hazard analysis=biztonsági veszélyelemzés):

A nagyobb mértékben kritikus rendszerek számára szükséges további biztonsági elemzés, abból a célból, hogy a PHA eredményeit finomítsák. A fejlesztési folyamat elõrehaladásával az elemzés mindinkább a követelményeket megvalósító alrendszerekre és komponensekre irányul. A veszélyeztetések feltárása többféle elemzési módszert is igényelhet.

Safety risk assessment (kockázat becslés):

Az SHA eredményeit hasznosító kockázatelemzés vizsgálja a különbözõ veszélyeztetések hatásait és megjelenési gyakoriságát vagy valószínûségét. Az SHA és a hozzá csatlakozó kockázatelemzés részleteit az **SHA jelentésben**, valamint a biztonsági naplóban rögzítik.[16]

Independent safety audit (független biztonsági audit):

A nagyon nagy mértékben biztonságkritikus rendszerek vizsgálata, ami a kockázatbecslés után következik. Az eredmények nem kerülnek a biztonsági naplóba, hanem a független biztonsági audit jelentésébe.

[16] Az itt szereplõ veszélyelemzések jelentõs részét például az egyedi, biztonságkritikus objektumok biztosítási díjának megállapításakor is el kell végezni.

Összegzésként megállapíthatjuk:
Minden rendszerre *elõzetes veszélyazonosítást* kell végezni és a veszélyek eredményeit az *elõzetes veszélyeztetési listába* kell rögzíteni.
Az elõzetes veszélyazonosítás után az *elõzetes veszélyelemzést,* a *biztonsági vizsgálatokat* a biztonságkritikus rendszerekre folytatni kell.
A nagyobb mértékben biztonságkritikus rendszerekben az elõzetes veszélyazonosítás, az elõzetes veszélyelemzés és a biztonsági vizsgálatok után a biztonsági veszélyelemzés és a kockázat becslés is elvégzendõ feladat, eredményei a biztonsági tervbe és a biztonsági veszélyelemzés jelentésébe kerülnek.
A *biztonsági napló* tartalmazza az elõzetes veszélyeztetési listát, az elõzetes veszélyelemzés jelentését, a biztonsági tervet és a biztonsági veszélyelemzés jelentését.
A nagyon nagy mértékben biztonságkritikus rendszerek vizsgálatához független biztonsági audit szükséges.

2.4. A kockázatelemzésnél és a hibafa elemzésnél alkalmazható matematikai módszerek

Shannon modell a hibafa elemzésnél; a rendszervizsgálat szempontjából döntéshozatalra alkalmas hibafák megszerkesztése a Shannon karakterisztikával lehetséges. A Shannon karakterisztika egy függvény, amelynek független változója a vizsgált rendszer vergõdési intenzitása, a függvényértéke a fõesemény valószínûsége. A Shannon-modellben egy mûszaki rendszer esetén vergõdésrõl beszélünk, ha a szóban forgó rendszer minden elemi eseménye véletlenszerûen, egyenlõ valószínûséggel és egymástól függetlenül változik. Ha ez a közös valószínûség értéke p, akkor p-t nevezzük a rendszer *vergõdési intenzitásának*. A Shannon modell szerint nem az a mûszaki rendszer tekintendõ abszolút biztonságosnak, melynek fõeseménye sohasem következik be, hanem az, melynek minden állapotában pusztán az állapot ismerete alapján eldönthetõ, hogy a fõesemény fennáll-e vagy sem. Ez a feltétel a Shannon modell szerint a biztonságra szükséges de nem elégséges. A Shannon modellben a rendszer abszolút biztonságának elegendõ feltétele, ha fõesemény valószínûsége megegyezik a rendszer vergõdési intenzitásával. Ezt az értéket döntési pontnak nevezzük, ebben a pontban a rendszer ideálisan viselkedik, tehát a hibafa ilyen esetben döntésképes helyzetet mutat fel.

Kvalitatív és kvantitatív kockázatelemzési eljárások:
A kvalitatív módszer nem kockázati mérõszámokat, hanem minõségi szinteket állapít meg, tehát olyan vagy hasonló fogalmakkal találkozhatunk, hogy a kockázat nagy, közepes vagy kicsi. Elõfordul, hogy az ilyen fogalmi meghatározásokat a döntéshozók nem tartják elég egzaktnak. A kvantitatív (mennyiségi) elemzés számszerûsíti a kockázati valószínûségeket, és a számokkal további elemzések, értékelések is végezhetõk. A fejlett informatikai rendszereket használó országokban a kvantitatív

módszertan az elfogadottabb, Magyarországon is egyre nagyobb az elvárás a kockázatelemzést végzõkkel szemben a mérhetõségre, a számszerûsítésre.

Új elméleti matematikai módszerek [15] is elõtérbe kerültek az utóbbi évtizedekben, amelyek újfajta, a bizonytalanságot is kifejezõ számokkal dolgoznak, ilyen például a fuzzy elmélet, az intervallum-analízis[19], a valószínûségi sávok[20], a hibrid aritmetika[21], ezeket a módszereket a különbözõ tudományterületeken egyre szélesebb körben alkalmazzák.

A fejezet további részében célul tûztem ki, hogy a kockázat meghatározására néhány eljárást említsek és részletesen bemutassam a fuzzy elmélet adaptálását, amely alkalmas arra, hogy a kockázatelemzésnél a kockázatra az elvárt számszerû adatokat szolgáltassa.

2.4.1. Fuzzy elmélet

A tudományterületek egy részénél az a cél, hogy egzakt matematikai modelleket építsenek fel a tapasztalati jelenségek megfigyelése alapján, majd ezeket a modelleket használják fel a valós dolgok jövõbeni viselkedésének meghatározására. A valós dolgok nem mindegyike sorolható be ezekbe a precíz modellekbe, mert többnyire valamilyen bizonytalan pontatlansággal rendelkeznek. A fuzzy elméletnek az egyik célja olyan módszerek kifejlesztése, amelyekkel szabályokba foglalhatók és megoldhatók azok a problémák, melyek túl bonyolultak vagy nehezen megfogalmazhatók a hagyományos vizsgálati módszerek segítségével. A fuzzy szó jelentése; homályos, elmosódott, lágy körvonalú, életlen vonalú. Innen származik a fuzzy logika elnevezés. A fuzzy logikát, illetve elsõ megfogalmazásában az ezzel algebrailag azonos felépítésû fuzzy halmazelméletet elõször Lotfi A. Zadeh Fuzzy Sets címû munkájában 1965-ben írta le. Segítségével a pontatlan vagy bizonytalan információkat, ismereteket matematikai formába lehet foglalni, és azokat kvantitatív módon lehet jellemezni. A fuzzy elmélet a halmazhoz tartozás szigorú definícióját kiterjesztve olyan módszert alkot, amely alkalmas a pontatlan, a becsült értékek kezelésére, a rosszul definiált fogalmak

---

[19] Intervallum-analízis (Moore 1979). A kiinduló adatok intervallumok, amelyek hossza a bizonytalanság mértékét fejezi ki. A valódi érték valahol az intervallumon belül helyezkedik el, de nem tudni, hol. Az intervallumokkal az összes szokásos aritmetikai mûveletet el lehet végezni.
Moore R. M. (1979). Methods and applications of interval analysis. SIAM Studies on Applied Mathematics. Vol. 2. Philadelphia

[20] Valószínûségi sávok (Ferson, Root, Kuhn, 1999). A kiinduló adat hibáját két eloszlásfüggvény közé esõ terület nagysága fejezi ki. A módszer nagy elõnye, hogy az adott tulajdonság eloszlásának jellegét is figyelembe veszi.
Ferson S., Root W., Kuhn R. (1999). RAMAS Risk Calc. Risk assessment with uncertain numbers. Applied Biomathematics. New York

[21] Hibrid aritmetika (Cooper, Ferson, Ginzburg 1996). Ez a módszer valós számok, intervallumok, fuzzy számok és valószínûségi sávok együttes értékelését teszi lehetõvé.
Cooper J. A., Ferson S., Ginzburg I. R. (1996). Hybrid processing of stochastic and subjective uncertainty data. Risk Analysis. 16. 785-791

matematikai leírására is. A nem jól definiált fogalmaknál (pl.: kicsi, közepes, nagy) a megfelelõ halmaz határait nem tudjuk egzakt módon meghatározni. Ebben az esetben az elemek halmazhoz tartozása nem minden esetben dönthetõ el egyértelmûen, így annak mértékét érdemes egy folytonos skála egy megfelelõ értékével jelölni. Minden elemhez egy skálaértéket rendelünk, amely megadja, hogy milyen mértékben tartozik az elem a halmazhoz. A kisebb érték azt jelenti, hogy a halmazt definiáló tulajdonság kevésbé jellemzõ az adott elemre, így a halmazhoz tartozása bizonytalanabb, mint a nagyobb értékû elemeké. Az A halmazhoz tartozás mértékét a halmazhoz tartozási függvény (μ) adja meg. Ezzel a függvénnyel megadott halmazokkal foglalkozik a fuzzy halmazelmélet.

A klasszikus halmazelmélet és logika szoros kapcsolatban áll, mivel a halmazhoz tartozás egy logikai értékkel jellemezhetõ. Ennek megfelelõen a fuzzy halmazelmélet kialakulásával létrejött a fuzzy logika is.

A fuzzy logika értelmezését és összehasonlítását a klasszikus matematikai logikával a következõ táblázat szemlélteti.

A klasszikus matematikai logika	Fuzzy logika
Legyen $\mathbf{A}=\{\mathbf{a_1},\mathbf{a_2},\ldots,\mathbf{a_n}\}$egy halmaz Kérdés: $\mathbf{a_i}$ eleme-e az **A** halmaznak?	
Válasz: hogy $\mathbf{a_i} \in \mathbf{A}$ vagy $\mathbf{a_i} \notin \mathbf{A}$ egyértelmûen eldönthetõ. Ha $\mathbf{a_i} \in \mathbf{A}$, akkor a válasz **igen**, az értéke **1** Ha $\mathbf{a_i} \notin \mathbf{A}$, akkor a válasz **nem**, az értéke **0** Az igazságtere: {0,1}	Válasz: a halmazba tartozás 0, illetve 1 értékei nem ennyire egyértelmûek, 0 és 1 közötti értékek is léteznek, amelyek megmutatják, hogy egy adott $\mathbf{a_i}$ elem mennyire tartozik bele a halmazba: nagyon, kissé, kevésbé, vagy egyáltalán nem. Igazságtere véges vagy végtelen számosságú, amelyben a logikai értékek fuzzy halmazok.
A hagyományos matematikai logikában azt az elemet, amelyhez 0-át rendeltünk, nem soroljuk fel a halmaz elemei között.	Minden **A** halmazbeli $\mathbf{a_i}$ elemhez hozzárendelünk egy általában 0 és 1 közötti számot, amely jellemzi az elem halmazba tartozásának mértékét. Tehát az **A** halmaz a fuzzy logikában az alábbi módon néz ki: $A = \left\{a_1^{(k_1)}, a_2^{(k_2)}, \ldots, a_n^{(k_n)}\right\}$A felsõ indexbe írt k_1, $k_2,\ldots,k_n$ értékek a halmazelemekhez rendelt, halmazba tartozást jellemzõ számot jelölik.
A következtetések precízek.	A következtetések közelítõk.
	Nyelvi változókat vezet be, amelyek értékei fuzzy kritériumok, és ezeket egy természetes nyelv szavaival fogalmazzák meg.

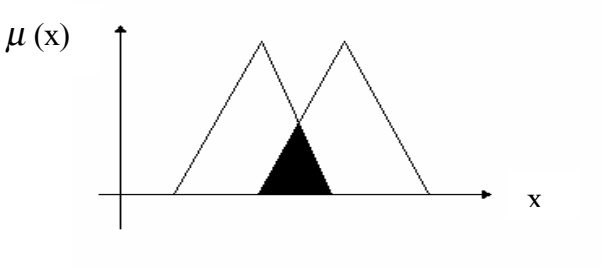
Bevezetjük a *tagsági függvény* fogalmát; μ az A halmazba tartozás mértékének megjelölésére, az alaphalmaz értékeihez rendel egy [0;1] intervallumbeli értéket. A legelterjedtebb tagsági függvény-forma a háromszög, de trapéz, harang görbe, fûrészfog is használatos. A függvény formájánál fontosabb az elhelyezett függvények száma és helyzete egy adott intervallumon. Háromtól hét függvényig általában elegendõ a bemenetei tartomány lefedéséhez.

Fuzzy mûveletek: [13]

Egy mûvelet fuzzy megfelelõje többféle módon is definiálható, az elemi mûveletek (konjunkció, diszjunkció, negáció, implikáció) definiálásánál az volt a cél, hogy a matematikai logikai mûveleteket speciális esetként magukba foglalják. Az elemi fuzzy logikai mûveleteket ki kellett egészíteni, hogy a természetes nyelv kifejezéseit modellezni lehessen. Fuzzy halmazokon a szakirodalom nagyon sokféle mûveletet értelmez, ezek közül csak az ún. elemi mûveletekkel foglalkozom.

1./ Két fuzzy halmaz AND (metszet) mûvelete az a halmaz, amely a két argumentum halmaz közös elemeit tartalmazza, minden elemet véve a legkisebb elõforduló beletartozási értéken.

$$\mu_{A\cap B}(x) = \min\left[\mu_A(x), \mu_B(x)\right]$$

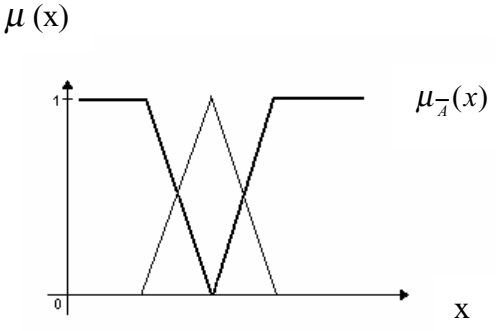


2./ Két fuzzy halmaz OR (unió) mûvelete az a halmaz, amely minden elõforduló elemet tartalmaz a lehetõ legnagyobb beletartozási értéken véve.

$$\mu_{A\cup B}(x) = \max\left[\mu_A(x), \mu_B(x)\right]$$

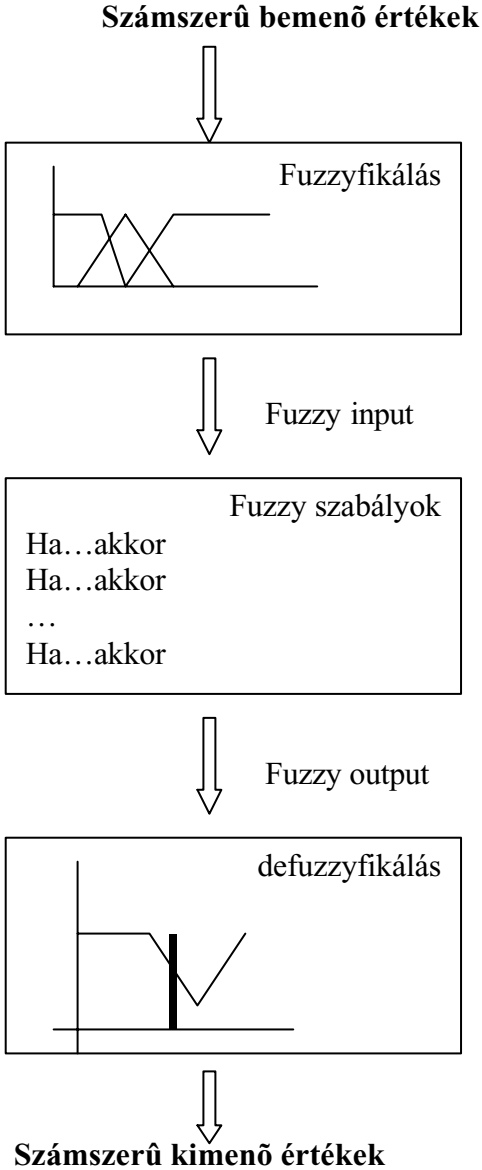
3./ Egy halmaz negáltján (komplementerén) azt a halmazt értjük, mely tartalmazza az összes elemet, de az eredmény halmaz elemeinek tagsági értékeit kivonjuk 1-bõl.

$$\mu_{\bar{A}}(x) = 1 - \mu_A(x)$$



A fuzzy logika és halmazelmélet szoros kapcsolatban áll, definiálhatók a halmazmûveleteknek megfelelõ logikai mûveletek is.

Egy fuzzy algoritmus felépítése:



- Fuzzyfikálás: a bemeneti értéket fuzzy értékre alakítja át, tehát meghatározzák az egyes input paraméterek tagsági fokát.
- Következtetés: Minden egyes kimenetre bemenetenként fel kell írni azokat a szabályokat, melyek azt a fuzzyifikált bemenetek egyes értékeinek megfelelõen létrehozzák. A szövegesen megfogalmazott szabályok alapján elõállítja a rendszer fuzzy típusú válaszát. A szabályrendszer feladata, hogy alkalmazza a szabálybázisban leírt szabályokat és létrehozza a kimeneti fuzzy típusú értékeket.
- Összeépítés: Az egyes kimenetek esetében egy halmazba össze kell fogni az összes szabályt, mely hat rá.
- Defuzzyfikálás: A kapott matematikai eredményt vissza kell alakítani számértékké. Tehát a defuzzyfikáció a fuzzy típusú kimeneti értékeket alakítja át kimeneti jellé.

2.4.2. A fuzzy elmélet felhasználása a kockázatelemzésnél

A kockázat meghatározásánál nagyon sokféle eljárást használnak, pl. a környezeti, a biztosítási, a befektetési vagy az informatikai kockázatnak vannak közös paraméterei, de sokban eltérnek egymástól.

- A *független fenyegetõ tényezõk* közel *teljes körû feltárásával* lehet eljutni a kockázat kiszámításához. A közel teljes körû feltárás azt jelenti, hogy a fenyegetõ tényezõk halmaza általában nem fedi le a teljes eseményteret, de arra kell törekedni, hogy ezeket a tényezõket mind teljesebben írjuk le. A teljes valószínûség tételét alkalmazva kapjuk a kockázat becslését:

$$P = P(A_1)P(K|A_1)+P(A_2)P(K|A_2)+ \ldots +P(A_n)P(K|A_n) = \sum_{i=1}^{n} P(A_i)\,P(K|A_i)$$

ahol $P(A_i) \neq 0$; $i \in N^+$

P - a kockázat valószínûsége

$P(A_i)$ - az i. fenyegetõ tényezõ bekövetkezésének a valószínûsége

$P(K|A_i)$ - az i. fenyegetõ tényezõ bekövetkezésekor keletkezõ kár feltételes valószínûsége

A kockázat ilyen módon való meghatározásának nagy elõnye a szilárd elméleti alap és a jól definiált fogalmak, de a gyakorlatban több probléma is felmerülhet:

- a teljes eseményrendszer megadásának a nehézsége,
- a kapott eredmények szövegesen nehezen értékelhetõk,
- sok valószínûséget kell meghatározni és megadni,
- valamilyen változás esetén az értékeket újra meg kell határozni.

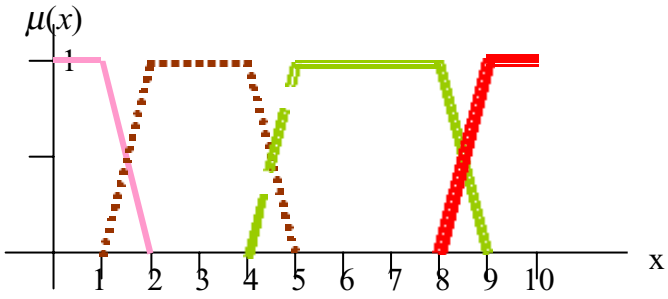
- Egy másik megközelítési mód szerint a *kockázatot a kár súlyosságának, valószínûségének, és a veszélynek való kitettség idõtartamának szorzataként határozhatjuk meg.* Természetesnek tûnik a kitettség idõtartamát figyelembe venni a veszélyes anyagok jelenlétében az emberek biztonságát és egészségét fenyegetõ kockázat meghatározásánál. Az informatikai rendszerek kockázatelemzésénél kevésbé gondolunk erre a tényezõre, pedig pl. az internethez való csatlakozás idõtartama növeli a számítógépes rendszerek fenyegetettségét. Mivel a gyakorlatban ezt a kockázat meghatározást kevésbé használják, így nincs kellõ tapasztalat a kitettség idõtartamának megfelelõ módon való figyelembe vételére.
- A kockázat meghatározása történhet kockázati mátrix létrehozásával is, az egyes fenyegetõ tényezõk kockázata a mátrix megfelelõ valószínûség és kár párosával megadható.
- A fuzzy algebra lehetõvé teszi, hogy a kockázatot alacsony, közepes vagy magas szintûnek jelöljük meg. [14] A fuzzy logikai módszert alkalmazó kockázatbecslési eljárások egy idõben több logikai szabályt (szabálybázist) alkalmaznak. A fuzzy logikával támogatott kockázatelemzésnél elsõ lépésként a szabálybázist és a hozzá kapcsolódó fogalmakat és kategóriákat kell definiálni, ez a kockázati mátrix, valamint a súlyossági és valószínûségi fogalmak meghatározását jelenti.

A szabálybázis meghatározása a kockázati mátrix felírásával:

A kár súlyossága	Elõfordulási valószínûségek				
	gyakori	valószínû	eseti	ritka	nem valószínû
katasztrofális	nm	nm	m	m	k
kritikus	nm	m	m	k	a
csekély	m	k	k	a	a
elhanyagolható	k	a	a	a	a

nm=nagyon magas m=magas k=közepes a=alacsony

A kár súlyossági kategóriának tagsági függvényei:

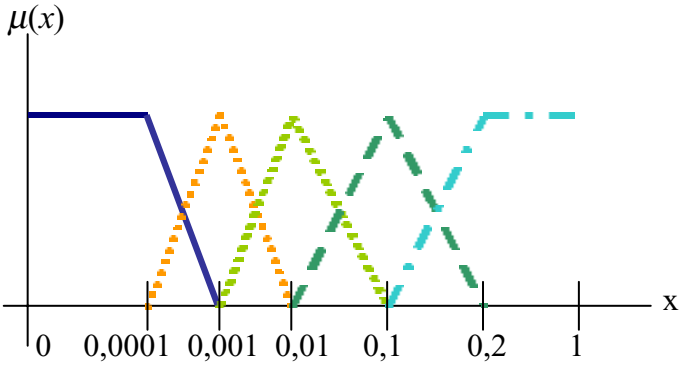


Jelölések:
elhanyagolható:
csekély:
kritikus:
katasztrofális:

A kár súlyosságát [0;10] skálán vettem fel.

2.12. ábra. A súlyossági kategóriák tagsági függvényei

Az elõfordulási valószí nûség kategóriák tagsági függvényei:

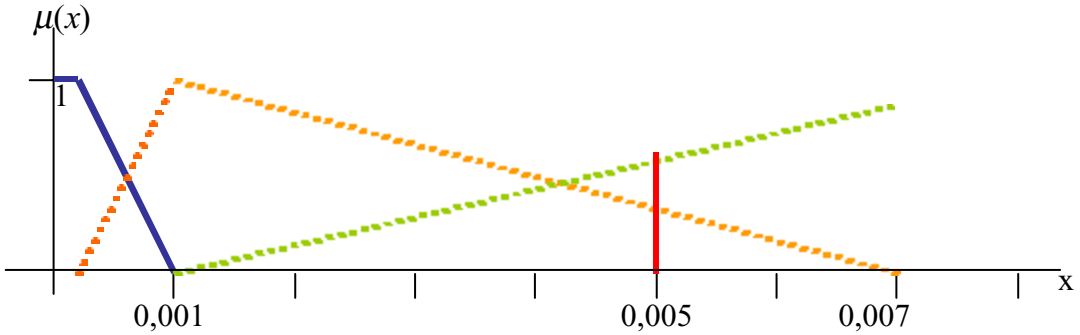


Jelölések:
nem valószínû:
ritka:
eseti:
valószínû:
gyakori:

A valószínûség kategóriái a [0;1] skálán.

2.13. ábra. A valószínûségi kategóriák tagsági függvényei

Ha a vízszintes tengelyen a beosztást egyenletesen vesszük fel, akkor a késõbbiekben grafikus megoldást is alkalmazhatunk. A pontosság érdekében célszerû egyenlettel is leírni a tagsági függvényeket:



2.14. ábra. A valószínûségi kategóriák tagsági függvényei, a 2.13. ábra egy részének nagyítása

A valószínûségi kategóriák tagsági függvényeinek egyenlettel való leírása:

nem valószínû:

$\mu_1=1$	a [0; 0,0001] intervallumban
$\mu_2=-1111{,}11x+1{,}11$	a [0,0001; 0,001] intervallumban

ritka:

μ_3=1111,11x -0,11 a [0,0001; 0,001] intervallumban

μ_4= -166,7x+1,17 a [0,001; 0,01] intervallumban

eseti:

μ_5=166,7x –0,17 a [0,001; 0,01] intervallumban

μ_6= -10,75x +1,08 a [0,01; 0,1] intervallumban

valószínû:

μ_7= 10,75x –0,08 a [0,01; 0,1] intervallumban

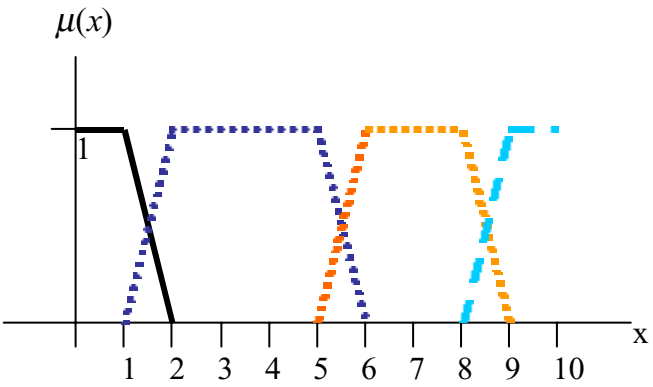
μ_8= -10x +2 a [0,1; 0,2] intervallumban

gyakori:

μ_9= 10x –1 a [0,1; 0,2] intervallumban

μ_{10}= 1 a [0,2; 1] intervallumban

Kockázati kategóriák:



Jelölések:

alacsony:

közepes:

magas:

nagyon magas:

A kockázat kategóriáit [0;10] skálán vettem fel.

2.15. ábra. A kockázati kategóriák tagsági függvényei

- Példaként tegyük fel, hogy a kár súlyosságának mértéke 4,75.

A tagsági függvények egyenletéből kiszámítható a fuzzy tagsági érték:

mivel x=4,75 és μ=x-4 —— μ=0,75

x=4,75 és μ=-x+5 —— μ=0,25

Tehát:

μ = (*súlyosság* = *kritikus*) = 0,75

μ = (*súlyosság* = *csekély*) = 0,25

Megjegyzés: amennyiben méretarányos grafikonnal adták meg a szakértők a tagsági függvényeket, akkor a meghatározás a grafikonról való leolvasással is történhet.

- Tegyük fel, hogy a valószínûség 0,005. A fuzzy tagsági érték kiszámítása:

Mivel x=0,005 és μ= -166,7x+1,17 —— μ=0,3

x=0,005 és μ= 166,7x-0,17 —— μ=0,7

Tehát:

μ = (*valószínûség* = *ritka*) = 0,3

μ = (*valószínûség* = *eseti*) = 0,7

Következtetés:

1. **Ha** a súlyosság kritikus **és** a valószínûség ritka, **akkor** a kockázat közepes.

$\mu(x)_k$= min(0,75;0,3)=0,3 (a már értelmezett **AND** mûvelet szerint, ld. 54. old.)

2. **Ha** a súlyosság kritikus **és** a valószínûség eseti, **akkor** a kockázat magas.

$\mu(x)_m$= min(0,75;0,7)=0,7

3. **Ha** a súlyosság csekély **és** a valószínûség ritka, **akkor** a kockázat alacsony.

$\mu(x)_a$= min(0,25;0,3)=0,25

4. **Ha** a súlyosság csekély **és** a valószínûség eseti, **akkor** a kockázat közepes.

$\mu(x)_k$= min(0,25;0,7)=0,25

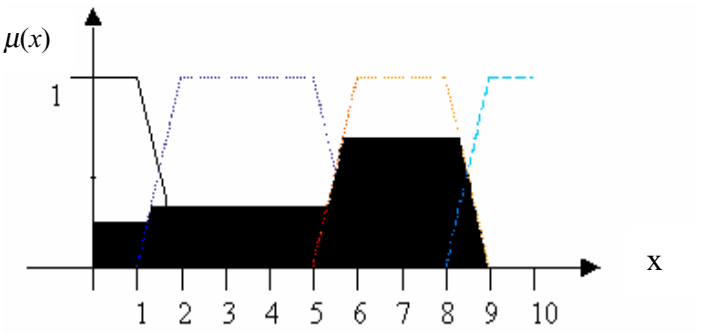
Összeépítés:

$\mu(kockázat = magas) = 0,7$

$\mu(kockázat = alacsony) = 0,25$

$\mu(kockázat = közepes) = 0,3$

(a szabályok szerint, ha többször kapjuk ugyanazt a következményt, akkor a maximálisat kell venni, **OR** mûvelet, ld. 54. old.)



A kockázati kategóriák tagsági függvényei ábrába berajzolom az összeépítés eredményét.

2.16. ábra. Az összeépítés eredménye

Defuzzyfikálás:

Többféle defuzzyfikáló eljárás használatos, amelyek egy numerikus értéket rendelnek a végeredmény fuzzy halmazához. A különbözõ eljárások más-más eredményt hozhatnak ki, a tagsági függvények formájának megváltoztatása kompenzálni tudja a defuzzyfikáció eltéréseit.

A maximumok súlyozott átlagának módszerével fejezzük ki a kockázat értékét:

$$K = \frac{\sum_{i=1}^{n} \mu_i x_i}{\sum_{i=1}^{n} \mu_i} = \frac{0,25 \cdot 0,85 + 0,3 \cdot 3,5 + 0,7 \cdot 7}{0,25 + 0,3 + 0,7} = 4,9$$

A fuzzy elméletnek a kockázatelemzésnél való alkalmazásának az elõnyeit a következõ pontokban foglalom össze:

- Lehetõség van a számszerû eredmények további felhasználására.
- A rendszer egyszerû felépítésû, a szabálybázis felépítése könnyen érthetõ.
- Precíz és pontatlanul definiált adatokat egyaránt tud kezelni.
- Szemléletmódja közel áll az ember napi valóság-szemléletéhez.

Hátránya, hogy elméletileg nem eléggé megalapozott.

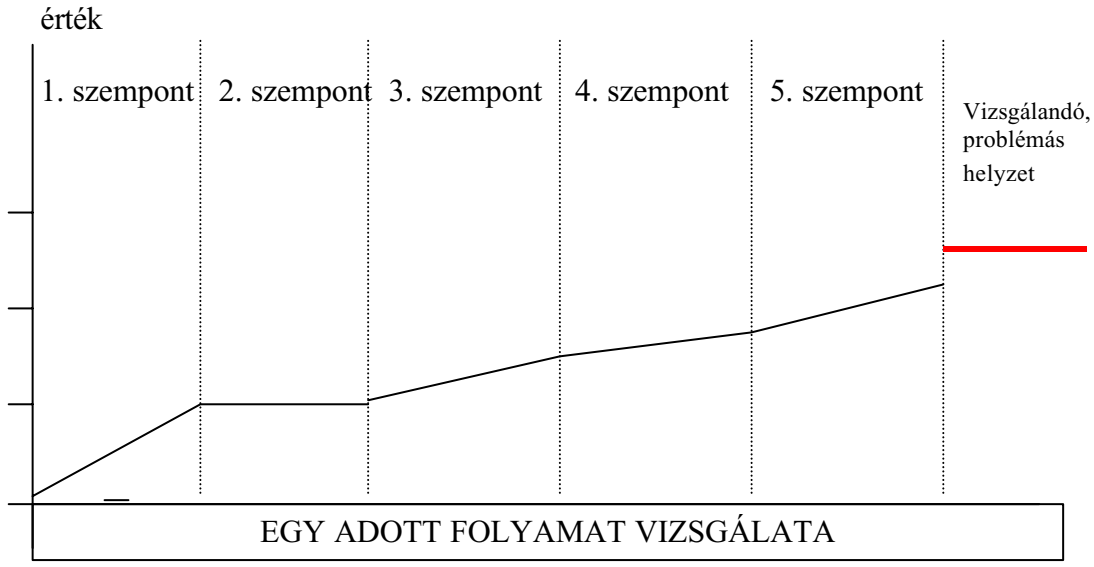
Összességében levonhatjuk azt a következtetést, hogy a fuzzy elmélet jól alkalmazható a kockázatelemzésnél. Azok a pozitív tulajdonságok, hogy a becsült valószínûségi és kárértékek jól kezelhetõk és egy konkrét számszerû kockázati értékhez is vezethetnek, mindenképpen az alkalmazása mellett szólnak.

2.5. Kockázatelemzési módszerek a védelmi szférában, a sajátosságok kiemelése

A Vám- és Pénzügyõrség az elmúlt években különbözõ kockázatelemzési rendszereket (nem informatikai kockázatelemzéseket) épített ki a bûnüldözési területen. [9]

- A Nyomozati és Szabálysértési Fõosztály folyamatosan végez kockázatelemzést, amely a bûnügyi adatok értékelésén a kockázati tényezõk és profilok kialakításán alapul.
- Különleges Ügyek Fõosztályán a bûnügyi felderítés érdekében elemzik az ügyfelek és a testületi tagok által elkövetett bûncselekmények különbözõ adatait.
- Központi Bûnüldözési Parancsnokság szervezetén belül 2000-ben megalakult a Bûnügyi Értékelõ és Elemzõ Osztály, amelynek feladata a bûnügyi adatok folyamatos figyelemmel kisérése, azok statisztikai elemzése, a várható trendek, elkövetési módszerek elõrejelzése.
- A határvámhivataloknál 1999 óta kutatócsoportok és egyes határvámhivataloknál (pl. Nagylak) kockázatelemzõ csoportok végzik a kockázatelemzõ tevékenységet. Kockázatelemzési program határozza meg, hogy milyen szállítmányokat érdemes ellenõrzés alá vonni, mivel minden határátlépõre a vámvizsgálat lehetetlen. A kockázatelemzési program meghatározott szempontok szerint választja ki a szigorúbb vagy akár tételes ellenõrzésre a határátlépõt.
- Központi Járõrszolgálat Parancsnokság (az operatív mobil egységeket mûködtetõ szervezet): Az e szervezetben mûködõ Ellenõrzés-felügyeleti és Koordinációs Osztály folyamatos információgyûjtést végez, amely egyfajta kockázatelemzés is.
- Központi Repülõtéri Parancsnokság: a Budapesti 1. számú Repülõtéri Vámhivatal kockázatelemzõ munkájának nagy részét az Operatív Csoport végzi.
- Ellenõrzési Igazgatóság: 1998 szeptemberében az Ellenõrzési Hivatalnál felállításra került egy – jelenleg még nem szervezetszerûen mûködõ – 4 fõs csoport, amelynek kizárólagos feladata az utólagos ellenõrzést elõkészítõ kockázatelemzés.

A kockázatelemzést, amely ellenõrzésre választja ki a határátlépõt, egy összefoglaló ábrán szemléltetem:



Például egy szállítmányt nagyon egyszerûsített módon öt szempont szerint vizsgálunk, minden szempontnak valamilyen értéket adunk. Ha az ötödik szempont után az értékek összege eléri a vizsgálandó helyzet szintvonalat, akkor a szállítmány további gyakorlati vizsgálata szükséges.

A katonai mûveletek, a modern hadviselés környezetszennyezéssel jár, szükségszerûvé vált a hadseregek és a környezet kapcsolatának átértékelése béke- ill. háborús idõszakokban. A különbözõ katonai mûveletek a környezet számára kockázatot jelentenek. Kockázatosnak minõsíthetõ egy környezeti esemény (x), ha a károsító hatás bekövetkezésének valószínûsége P(x) jelentõs és a keletkezett hatás, az okozott kár D(x) is egy meghatározott szintet elér. Egy környezeti esemény kockázata megközelíthetõ és kifejezhetõ a következõ formában: $R(x)= P(x) \circ D(x)$. Ez a megközelítési mód, ami a biztosítók klasszikus szemléletmódja, csak a gyakran bekövetkezõ kockázati események esetén szolgáltat jó eredményt, az egyedi jelenségek modellezése másképp történik.

Ha a különbözõ *békefelkészítési mûveleteket* vizsgáljuk, ezek a környezetre más-más jellegû igénybevételt jelentenek. A hatékony környezeti kockázatkezelés érdekében – figyelembe véve az egyes mûveletek tartalmát – különbözõ felkészítési formákat kategorizálnak. A környezeti kockázatelemzés alapja az egyes felkészítési formák katonai mûveleti folyamatainak környezeti tartalma, amelyet meghatároz a gyakorlat helyszíne, idõtartama, a gyakorlatba bevont személyek száma, az alkalmazott haditechnika (eszközök, anyagok) [10].

Fontossá válhat a szennyezett területek kockázatelemzése, ami figyelembe veszi az adott terület tényfeltárásra támaszkodó részletes vizsgálatát, a környezetre, az emberre elviselhetõ szint meghatározását, a kármentesítési célállapotot. Számos helyen található leromlott állapotú, a környezetre is veszélyt jelentõ laktanya és volt katonai létesítmény.

Az elemzés után itt is sor kerülhet a terület kármentesítésére, a hasznosítatlan épületek bontására vagy felújítására.

A védelmi szféra informatikai rendszereire sokan próbálnak bejutni, a behatolási szándékot sokféle dolog motiválhatja; bizalmas, titkos információk megszerzése, szabotázs, a meglevõ adatok megsemmisítése, megváltoztatása vagy bizonyos szolgáltatások blokkolása, a számítógépek kapacitásának kihasználása vagy egyszerûen a védelem kipróbálása. A lakosságra tartozó információk elhallgatása is indukálhat ilyen behatolást, civil szervezetek pl. környezetvédõk nem nevezhetõk illetéktelennek, hiszen bizonyos kockázatok megítélésében nagyon is illetékesek, de ha bejutnak a védelmi szféra valamilyen informatikai rendszerére, akkor hozzájuthatnak nem rájuk tartozó adatokhoz is, tehát a nyilvánosságra tartozó adatok visszatartása is lehet veszélyforrás. A külsõ és belsõ bejutási kísérletektõl is meg kell védeni ezeket az informatikai rendszereket. A megfelelõ védelem mellett az állandó ellenõrzés is szükséges. A felülvizsgálatot, a kockázatelemzést végzõk újabb veszélyforrást jelenthetnek. Magasabb vezetõi szint dönti el, hogy ki végezhet informatikai auditot, külsõ cég vagy csak a védelmi szféra informatikai szakemberei.

A NATO biztonságpolitikai rendszerében az egyik legfontosabb elem az információbiztonság. A NATO információbiztonsági politikája megalkotásánál a fenyegetõ tényezõk, a sebezhetõ pontok meghatározásából indul ki. Alapelve, hogy az információvédelmi rendszer elemeit úgy kell tervezni, hogy a rendszeren való áthatolás költsége, a ráfordított energia nagysága haladja meg a megszerezni kívánt információ értékét.

Fenyegetõ tényezõknél kiemelhetõ a NATO stratégiából a következõ gondolat „…állami és nem állami ellenfelek megpróbálhatják kihasználni a Szövetség függõségét az információs rendszerektõl úgy, hogy információs mûveletekkel mûködésképtelenné teszik a rendszereket.”[5]

A NATO Tudományos Ügyek Osztálya által kiadott útmutató egyik fejezete - A biztonsággal összefüggõ civil tudomány és technológia – foglalkozik a kockázatértékelés kutatási programjával, a kockázatértékelési módszerek tökéletesítésének és új eljárások kidolgozásának célkitûzésével [11].

A NATO AQAP-170[22] kiadványának C mellékletében kockázatelemzés, a kockázat kiértékelése, az ellenõrzés feladatai, módszerei szerepelnek [12].

A kockázat kiértékelése, becslése, elemzése a következõ lépésekbõl állhat:

Veszélyazonosítás, veszélyelemzés.

A különbözõ kockázati tényezõk közötti összefüggések feltárása, vizsgálata, a tényezõk rangsorolása.

A fejlesztés kockázatkezelési terve.

Kockázatok számításának, csökkentésének lehetõségei.

[22] AQAP-170: Allied Quality Assurance Publication, Szövetségi Minõségbiztosítási Kiadvány

Kockázati információk feldolgozása, a fejlesztési lehetõség jelzése.
A kockázatkezelés adatbázisának karbantartása.
Kockázati jelentések bemutatása a megfelelõ szakértõi fórumon.
A kockázati információk elõrejelzése.

A kockázatok azonosítása:

Az azonosítás általában a következõ területeket foglalja magába:
Kockázatok azonosítása, osztályozása, kategorizálása, az elõidézõ okok keresése, a kockázatok közötti összefüggések feltárása.
A potenciális kockázatok azonosításához különbözõ eszközök használhatók (kérdõívek, elemzések,…)
A teljes kockázat fogalomköre magába foglalja az azonosított, az elfogadható, a nem elfogadható, a nem azonosított és a maradvány kockázat fogalmát.

2.6. Összegzés

Az informatikai biztonság nem statikus állapot.
Egy informatikai rendszer biztonságának vizsgálatát az életciklusa során három nagyobb részterületre bonthatjuk. Az elsõ részben a rendszer létrehozásakor a biztonsági követelmények kidolgozásánál egy egyszeri tevékenységet végzünk. A második részterületnél a környezet és a követelmények folyamatosan változnak, így a kialakított biztonsági rendszert idõrõl idõre felül kell vizsgálni, csak így derülhet fény a jelen lévõ vagy az éppen kialakuló kockázatokra. A harmadik szegmens a jövõ megítélése, az új fenyegetések prognosztizálásával lehet a védelmi intézkedések tervezése, kidolgozása. Az elõrejelzés bizonytalanságának növekedése az idõtõl nagy mértékben függ.
A prognosztizálás bizonytalansága miatt fontos a rendszer idõszakos felülvizsgálata, a kockázatelemzés, amelynek során az informatikai rendszer aktuális mûködési biztonságáról szerezhetünk információt. Nagyszámú kockázatelemzési módszer létezik, vannak egész témakört átölelõ és sajátos alkalmazási területre kifejlesztett eljárások. Ezeket az eljárásokat kell alkalmassá tenni, kiegészíteni vagy ilyen eljárást kell kialakítani az adott informatikai rendszerekre történõ alkalmazáshoz.
A legalkalmasabb kockázatelemzési módszer kiválasztása és az adott rendszerre való alkalmazása nehéz feladat, a már sikeres módszertanok felhasználásával kialakítható az adott szituációra alkalmas eljárás. A szakirodalomban eddig megjelent módszertani útmutatók is felhasználják, tovább fejlesztik az elõzõeket. Például a Courtney módszer szerinti kockázati mátrix szinte változatlan formában elõkerül több eljárásban is, mint például a CRAMM-ben és az ITB 8. számú ajánlásában. Amennyiben valamilyen már

meglévõ ajánlás, módszertan alkalmazása a cél, akkor az egyes eljárásokat ismerni és különbözõ szempontok szerint értékelni kell, ez elõsegíti a megfelelõ módszer kiválasztását. Ha egy sajátos területre speciális kockázatelemzési eljárást kell kialakítani, akkor is ajánlatos több eljárás ismerete, így a pozitívumok beépíthetõk, a negatívumok kikerülhetõk.

Ebben a fejezetben kockázatelemzési módszereket mutattam be, kiemeltem az egyes módszerek erõsségeit és gyengeségeit, elõre kiválasztott szempontok szerint összehasonlítottam a bemutatott eljárásokat. *Az összehasonlító elemzést és értékelést tudományos eredménynek tekintem, egyrészt ezen elemzés felhasználásával dolgoztam ki a védelmi szféra informatikai rendszereinek kockázatelemzésére alkalmazható módszertant, másrészt az eredmények mások által is tovább hasznosíthatók és más módszertan megalapozására is felhasználhatók.*

3. Módszertani útmutató a védelmi szféra informatikai rendszereinek kockázatelemzéséhez

A második fejezetben öt kockázatelemzési módszert választottam ki és értékeltem. Felvetõdik a kérdés, hogy a nagyon sok pozitív tulajdonsággal rendelkezõ módszerek mellett, miért készítek egy új kockázatelemzési módszertant a védelmi szféra informatikai rendszereinek vizsgálatára. Indoklásul kiemelem azokat a legfontosabb okokat, amelyek megerõsítették azt az elhatározásomat, hogy egy új módszertant kidolgozzak.

A COBIT meghirdetett célja az informatikai és üzleti célok összehangolása. Magyar nyelven hivatalosan nem jelent meg, a fordítás folyamatban van. Az eljárásnak nagy a felhasználtsága, mert általánosan alkalmazható, a célterülettõl függetlenül. A túl általános módszer nem jól alkalmazható a védelmi szféra sajátos informatikai rendszereinek elemzésére.

A CRAMM bizalmas, de nem titkos rendszerek vizsgálatára alkalmas – hirdeti önmagát, továbbá a CRAMM, az ITB 8. számú ajánlás és az IT-Grundschutzhandbuch elsõdlegesen a közigazgatás informatikai rendszereinek vizsgálatára készült.

A MARION biztonságra és kockázatra vonatkozó megállapításai erõsen függnek az elemzõk személyétõl, a vizsgálat megismétlésekor nem biztos, hogy ugyanazt az eredményt adják.

Feltétlen meg kell említeni; a védelmi szféra informatikai rendszereit más rendszerektõl eltérõ, újabb fenyegetõ tényezõk is veszélyeztethetik, amelyeket az elemzés során figyelembe kell venni.

Az okok közül ezek voltak a legmeghatározóbbak, amelyek miatt indokoltnak tartottam egy olyan kockázatelemzési módszertan kidolgozását, amely a védelmi szférában alkalmazható.

Egy rendszer informatikai biztonságának megteremtését nem tekinthetjük megoldott, lezárt folyamatnak. Az informatikai rendszerben és a környezetében történõ állandó

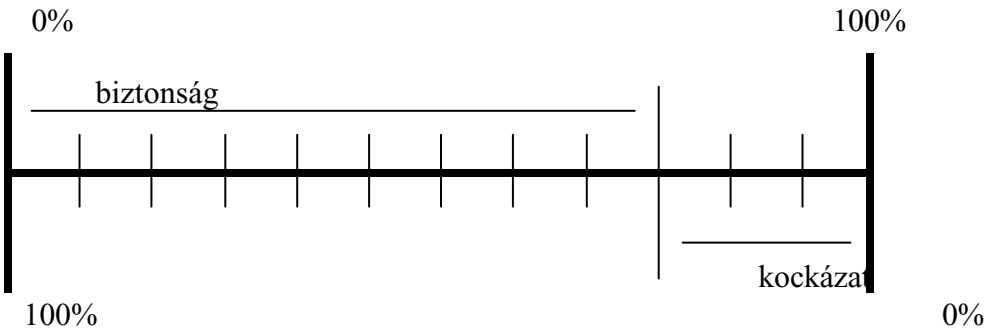
változás szükségessé teszi a rendszeres felülvizsgálatot, ellenõrzést és változtatást. Az informatikai kockázatkezelés területén az a cél, hogy ismereteink legyenek az értékeket fenyegetõ veszélyekrõl, azok valós nagyságáról és ennek megfelelõen kialakítható legyen az elégséges biztonság az adatok és a rendszerek számára.
Egy informatikai rendszer kockázatelemzésére kétféle módon kerülhet sor;

- a belsõ ellenõrzés részeként, amely során a felsõ vezetés utasítására megvizsgálják a rendszer egy részét vagy egészét, egyes folyamatokat, tevékenységeket. A cél az informatikai rendszer helyes mûködésének igazolása, vagy hiányosságainak feltárása, egy informatikai projekt végrehajtási módjának, eredményeinek kiértékelése lehet.
- a külsõ auditálás, kockázatértékelés részeként.

A kockázatelemzés az egész rendszert, annak egy részét, folyamatát vagy esetleg csak egy rendszer-elemet is érinthet. Pl.;

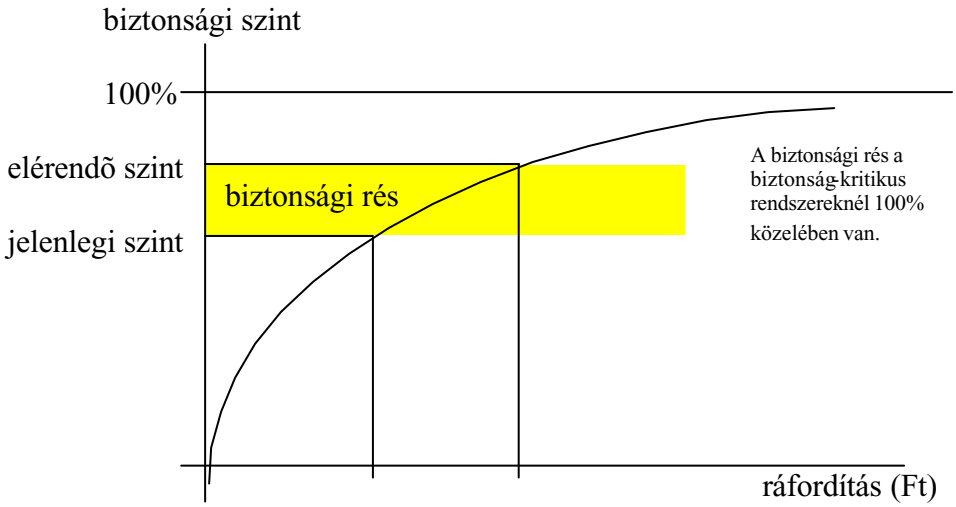
- új, komplex rendszerek beállításának utólagos vizsgálata,
- az informatikai eszközök fizikai átvizsgálása,
- alkalmazási rendszerek utólagos elemzése, alkalmazások értékelése,
- felhasználói programrendszer vizsgálata,
- felhasználói programok vizsgálata,
- rendszertervezési és -szervezési munkák elemzése,
- a dokumentált eljárások betartásának ellenõrzése,
- különbözõ szervezeti problémák vizsgálata,
- egy-egy számítógépes folyamat elemzése,
- hardver, vagy szoftver megbízhatóságának vizsgálata,
- rendszer-összeomlások, csalások, nagyobb hibák, támadások vizsgálata,
- hálózat, hálózati eszközök értékelése,
- a szerver operációs rendszerének értékelése,
- adattárak, adatbázisok értékelése,
- internetes és kapcsolt szolgáltatások elemzése,
- üzemeltetési eljárások értékelése,
- kapcsolódó rendszerek értékelése.

Ezeken kívül más szempontok is elõfordulhatnak a gyakorlatban. Nagyban befolyásolja a végzett munkát az, hogy milyen mélységû és mekkora területet ölel fel a kitûzött feladat. Az informatikai biztonság nem teremthetõ meg egy vagy több szolgáltatás, audit megvásárlásával, hanem a szervezet életébe beépülõ folyamatnak kell lennie. A 100%-os biztonság elérése is lehetetlen, összhangba kell hozni valamilyen módon a biztonságot és a kockázatot, amelyeknek a viszonyát a 3.1. ábrán szemléltetem;



3.1. ábra. Biztonság és kockázat

A következõ grafikonnal a biztonsági szint és a ráfordítás közötti kapcsolatot ábrázoltam.



3.2. ábra. Biztonság és ráfordítás

A biztonság-kritikus rendszereknél, a védelmi szféra egyes területeinél nagy ráfordítással érhetõ el a 100%-ot megközelítõ biztonsági szint. Specifikus kockázatelemzési módszerek használhatók a vizsgált terület sajátosságainak megfelelõen. Minden esetben a terület sajátosságainak figyelembevételével történik a legalkalmasabb módszer kiválasztása, kidolgozása.

A megfelelõ módszer kidolgozásánál figyelembe kell venni a következõket;

- a módszernek alkalmasnak kell lenni az adott rendszer elemzésére,
- tudományosan igazolhatónak kell lennie,
- olyan eredményeket kell szolgáltatnia, amely lehetõvé teszi, hogy a kockázatelemzés után a kockázatkezelést is el lehessen végezni,
- megismételhetõ legyen,
- felhasználóbarát legyen,
- a gyakorlatban a kockázatok meghatározásánál elõfordulhat, hogy a kockázatelemzést elegendõ olyan mélységben elvégezni, hogy az döntés-elõkészítõ információt hordozzon a védelmi intézkedések kiválasztásához, az egyes veszélyforrások esetén vizsgálják a hatásmechanizmusukat és a

különbözõ biztonsági tényezõkre gyakorolt hatásukat direkten próbálják meghatározni. A kockázati kategóriákat ezután a legmarkánsabb tényezõbõl származtatják.

- Más körülmények között elõfordulhat, hogy többlépcsõs, bonyolult mátrixok felírását igénylõ részletes vizsgálatot kell végezni.

Mindezek figyelembe vételével dolgozom ki azt a kockázatelemzési módszertant, amely a védelmi szféra informatikai rendszereinek vizsgálatánál használható.

3.1. Kockázatelemzés egyes lépéseinél használt eszközök

A kockázatelemzést végzõ személynek vagy csoportnak nagyon sok információra van szüksége a rendszer és a biztonságot fenyegetõ tényezõk minél részletesebb megismerése érdekében. Ezt a feltáró munkát számos eszköz támogatja, nem célszerû ragaszkodni egy-egy, a szakirodalomban ajánlott módszerhez, mivel minden informatikai rendszer más és más módon ismerhetõ meg. A következõkben néhány olyan eszközzel foglalkozom, amelyeket jó hatásfokkal fel tudunk használni.

3.1.1. A kapcsolattartást elõsegítõ eszközök

Kérdõívek:

Mint minden felmérésnél, a kockázatok meghatározásánál is kézenfekvõ módszer a kérdõívekkel történõ adatfelvétel. Jól szerkesztett kérdõívekkel sok fontos információ szerezhetõ be a rendszer folyamatainak feltárására, a rendszer struktúrájának megértésére, a rendszer és a környezet kapcsolataira vonatkozó adatok beszerzésére.

A megfelelõ kérdõívek megszerkesztése és a kiértékelés nagy figyelmet kíván. A kérdõívek szerkesztésénél a következõket kell figyelembe venni:

- A kérdések megfogalmazása egyszerû és érthetõ legyen.
- A kérdések rövidek, célratörõk legyenek.
- A vizsgálni kívánt résztémák logikus sorrendben jelenjenek meg a kérdõíven.
- Egy-egy résztéma kérdései egy csoportban legyenek, esetleg külön megjelölve.
- A kérdõív elején egyszerûbb kérdések szerepeljenek, és fokozatosan térjünk át a bonyolultabbakra.
- Zárt kérdéseknél a kérdõív szerkesztõje elõre megfogalmazza a lehetséges válaszokat.
- Nyitott kérdések esetében a válaszadó a véleményét a saját szavaival fogalmazza meg. Az ilyen válaszok értékelése nehézkes, de elõfordulhat, hogy más információt is megtudunk, mint az elõre megfogalmazott válaszok esetén. A nyitott, elgondolkodtató kérdéseket általában célszerû a kérdõív végén elhelyezni.

Jelentések, nyilvántartások vizsgálata:
A kifejezetten a kockázatkezeléshez tartozó iratanyag mellett értékelni kell számos más dokumentumot is, mivel tartalmazhatnak felhasználható elemeket.
Statisztikai elemzések vizsgálata:
A statisztikai elemzések használatának elõfeltétele egy olyan belsõ információs rendszer kialakítása, amely pontosan rögzíti a kockázatkezeléshez szükséges adatokat. A statisztikai elemzések fõ tárgya a valószínûségek megállapítása és az egyes jelenségek idõsoros bemutatása. A munka kezdetén a károk valószínûsége csak durván becsülhetõ, de az egyes kockáztatott elemekre vonatkozó jelleggörbéket a szakirodalomból és az általános statisztikai adatokból megállapíthatjuk. Az idõsorba rendezett adatok, akár grafikusan, akár táblázat formájában nagyon jól mutatják a változások irányát, jól értékelhetõvé teszik az egyenletesen növekvõ, csökkenõ tendenciákat, az értékek változásának határait és az egyszeri kiugró értékeket is. Megfelelõ vizsgálattal kimutathatók a változás törvényszerûségei is, megállapítható, hogy mi tekinthetõ véletlen ingadozásnak és mikor állunk szemben strukturális törésekkel.
Helyszíni vizsgálatok:
A helyszíni vizsgálatok a kockázatkezelést végzõk személyes, elsõ kézbõl való tájékozódását jelenti, amelynek nagyon sokféle oka, célja lehet. A helyszíni szemle lehet adatfelvétel, információszerzés, ellenõrzés, megfigyelés stb. Lehetséges, hogy az elemzést végzõ nyíltan végzi munkáját, vagyis közli a helyszíni szemle céljait, módszereit, elmondja, hogy mi teszi eljárását szükségessé, és azt, hogy milyen eredményeket vár. Mivel az informatikai biztonság fenyegetõ tényezõi között az emberi tényezõk vizsgálatának elsõbbsége van, így sokszor célszerû a vizsgálatra vonatkozó információkat nem feltárni.
Folyamatábrák:
A folyamatábrák elsõsorban a vizsgált rendszer megértésére, rendszerezésére készülnek. Pl. szemléletesen ábrázolható az adatáramlás iránya, az egymással kapcsolatban levõ rendszerelemek viszonya.

3.1.2. A kockázatértékelés áttekinthetõségének segítése

A kockázatértékelés egy nagyon bonyolult, szerteágazó tevékenység, ezért célszerû egy áttekintõ vázlatot, ûrlapot készíteni, amely tartalmazza a leglényegesebb ismereteket a rendszerrõl és a már elvégzett munkával kapcsolatos eredményekrõl, az esetleg azonnal meghozandó intézkedésekrõl. Az áttekintõ ûrlap tartalmazza a következõket:
- azokat a tényezõket, idevonatkozó szabályzatokat és útmutatókat, amelyeket mindenképpen figyelembe kell vennie a kockázatértékelésnél,
- a kockázatértékelési eljárás vázlatát,
- az értékelési munkát végzõk nevét, elérhetõségét, az elvégzendõk felosztását a team egyes tagjai között,
- a vizsgálat kezdetének és a befejezésnek a várható idõpontját,

- tevékenységek leírását,
- kockázatokat,
- a teendõ intézkedéseket,
- megjegyzéseket; a vizsgálat során felmerült fontos gondolatokat, megoldandó tevékenységeket.

3.1.3. Az informatikai rendszer megismerésének eszköze

Egy informatikai rendszert megismerni nem kizárólagosan az itt megadott módon lehet, az interjú egy lehetséges mód, ami abban is segítséget adhat, hogy más módszerrel milyen részletességû ismereteket kell szerezni.
A rendszer megismeréséhez alkalmazható interjú kérdései[23]:
Részletesen az 6. számú mellékletben.

1. Az adott szervezetre vonatkozó adatok (név, cím, telefonszám, fax, e-mail cím).
2. A kapcsolattartó adatai (név, beosztás, telefonszám, e-mail cím).
3. A szervezet tevékenységi területei. A tevékenységek besorolását ajánlatos a TEÁOR (Tevékenységek Egységes Ágazati Osztályozási Rendszere) szerinti kódszámok használatával kiegészíteni. Az 1998. január elsejével bevezetett új változata teljes mélységben, szerkezetében és tartalmában megegyezik a NACE Rev. 1-gyel. A besorolás 4 számjegyû. A TEÁOR rovatban, a besorolásnak megfelelõ 4 számjegyû kód alkalmazása szükséges.
   NACE Rev. 1. (Nomenclature générale des activités économiques dans les Communautés Européennes) Az EK-ban a gazdasági tevékenységek egységes statisztikai osztályozási rendszere. Alkalmazása a tagországok számára 1993-tól kötelezõ a 3037/90(EGK) sz. tanácsi rendelet és a módosítását elrendelõ 761/93(EGK) bizottsági rendelet alapján.
4. A szervezet felépítése:
   A szervezeti felépítést a könnyebb áttekintés érdekében úgynevezett organogrammal szokták ábrázolni. Általában a szervezeti struktúra grafikus megjelenítése szerepel az adott szervezet honlapján. A jól szerkesztett organogramból leolvasható a szervezet körülbelüli nagysága, kapcsolatainak rendszere.
5. Létszámadatok: A szervezet teljes létszáma, az informatikai rendszert használók létszáma.
6. A szervezet külsõ kapcsolatainak jellemzése: A kérdéseknek mennyiségre, fontosságra, az elektronikus kapcsolattartás milyenségére kell utalni.
7. Külsõ szolgáltatók által ellátott tevékenységek felsorolása.
8. Helyszínek és telephelyek létszámadatokkal.
9. A minõségirányítással kapcsolatos kérdések egyrészt az ISO 9000-es szabványsorozat szerint akkreditált tanúsítványra és annak érvényességi

[23] Az interjú kérdései a BS7799:1999 szabvány követelményeinek figyelembevételével készültek.

határidejére, másrészt különbözõ szabályzatok és stratégiák meglétére vonatkoznak, mint az iratkezelési szabályzat, IT stratégia, védelmi politika, mentési stratégia, helpdesk rendszer. Az iratkezelési szabályzat az iratok, a bármely technikai eljárással készült kép- és hangfelvételek, valamint a gépi adatfeldolgozás során keletkezett adathordozók biztonságos õrzésének módját, rendszerezését, nyilvántartását, segédletekkel ellátását, irattárba helyezését, selejtezését szabályozza. Az informatikai stratégia, annak hivatalos, megfogalmazása, hogy a szervezeten belül (vagy annak egy részében) az informatika milyen szerepet tölt be. A védelmi politika területe széleskörû. Foglalkozik a fizikai környezet védelmével (területek, berendezések, munkahelyek védelme), a hozzáférés szabályozásával (felhasználók felelõssége, hálózati hozzáférés, operációs rendszerhez való hozzáférés, alkalmazáshoz való hozzáférés, távmunka), személyekkel kapcsolatos védelemmel, a rendszer fejlesztésével és karbantartásával, megfelelõséggel (jogi követelményeknek, szabályzatokban megfogalmazottaknak), az információvagyon osztályozásával és kezelésével, a kommunikáció és mûködés irányításával (felelõsségi körök, rendszertervezés, védelem rosszindulatú szoftverek ellen, rendszerüzemeltetés, hálózatkezelés, adathordozók kezelése, információcsere, szoftvercsere), védelmi szervezettel (beleértve az információvédelmi infrastruktúrát, harmadik fél általi hozzáférés biztonságát, és az outsourcingot[24]). Minden rendszernek, vállalkozásnak szüksége van biztonsági mentésre az adatairól, lényeges a jól mûködõ mentési rendszer kidolgozása. A helpdesk segítségkérést jelent, a szervezetek által fenntartott ügyfélszolgálati funkció, ahol az ügyfelek valamilyen kommunikációs csatornán vagy csatornákon (telefon, fax, e-mail, web-es szoftver) közvetlen segítséget kaphatnak.

10. IT és adatkezelés helye a szervezetben: A kérdések az adott szervezetben az IT-vel foglalkozó egységekre, személyekre vonatkozik.
11. Sajátos feladatok, tevékenységek: A szervezet tevékenységi körére, a tevékenységek szervezeten belüli fontosságára és ezek IT támogatottságára vonatkoznak a kérdések.
12. A szervezeti IT rendszer sajátosságainak feltárása.
13. Kérdések az adatok veszélyeztetettségének felméréséhez.

3.1.4. A vizsgált szervezet tevékenységeinek megismerése és a tevékenységek osztályzása

Meg kell állapítani azokat a kritériumokat, amelyek alapján a tevékenységeket a késõbbiekben osztályozni fogjuk, és amelynek alapján megállapítjuk, hogy milyen információra van szükség minden egyes tevékenységre nézve. Az elsõ kérdõív kitöltésével a szervezet tevékenységi területeinek rangsor szerinti felsorolása már

[24] outsourcing: erõforrás kihelyezés

megtörtént, de a felsoroláson és a TEÁOR kódon kívül több információra is szükségünk van:

- A szokásos feladatok, idõtartamuk és gyakoriságuk. Az alaptevékenységen kívül van-e egyéb, ritkán végzett feladat?
- Hol végzik a tevékenységet? Kik végzik a feladatokat?
- Az adott tevékenység végzéséhez milyen képzettségre van szükség? Az egyes személyeknek megvan-e a szükséges képzettségük, megfelelnek- e az elõírásoknak?
- Törvények, határozatok és szabványok követelményei a végzett tevékenységgel kapcsolatban.
- A különbözõ biztonsággal kapcsolatos eseményekre reagáló figyelési adatok: nemkívánatos események, eddigi tapasztalatok, amelyeket a szervezeten belüli vagy rajta kívülrõl származó információból lehet megszerezni.
- Az eddig végzett tevékenységekre vonatkozó értékelések megállapításai.

A tevékenységek osztályzása:

El kell készíteni a tevékenységek listáját és csoportokba kell ezeket foglalni, egy a célnak megfelelõ kritérium szerint. A tevékenységek osztályozásának lehetséges módja;

- fontossági sorrend az informatikai biztonság szempontjából,
- fontossági sorrend a kár mértéke szerint,
- földrajzilag meghatározott területek tevékenységei.

3.1.5. Az informatikai biztonságot fenyegetõ tényezõk feltárásának lehetõségei

Hogyan lehet a veszélyforrásokról információt szerezni?

- Szabványok, munkahelyi belsõ szabályzatok, technológiai utasítások vagy leírások betartásának vizsgálatával. (Az alapfolyamatokra - adatvédelem és adatbiztonság - vonatkozó szabályzatok egyértelmûen rögzítik a kezelõszemélyzet tevékenységi körét, jogosultságait, felelõsségét, ellenõrzési rendszerét. A rendszerfolyamatokra - IT rendszer és IT szervezeti folyamatok - vonatkozó szabályzatok írják elõ a kezelõszemélyzet adatokkal való kapcsolatba kerülésének minimumát és maximumát.)
- A munkahelyek közzétett adatainak, tapasztalatainak, gyakori szakmai szokásoknak a tanulmányozásával, a munkavállalók vagy képviselõik tapasztalatainak értékelésével.
- A tudományos és mûszaki irodalom állandó figyelésével, a munkatevékenység, munkafolyamatok, technológiák, munkaeszközök, munkamódszerek közvetlen megfigyelésével.
- A már szükségtelen adatok tárolásának, megsemmisítésének ellenõrzésével.
- A beléptetõ rendszerek vizsgálatával, a biztonsági érzékelõk (behatolás, lopás, betörés, füst, tûz stb.) figyelésével.
- Helyszíni vizsgálatokkal és mérésekkel, amelyek során a következõket figyelik;
  illetéktelenek az informatikai rendszer közelében,

a tárolt adatokról történõ biztonsági másolat példányszáma és tárolási helye,
a különlegesen fontos berendezések tárolása,
a hálózat fizikai védelme (különösen nagy a veszély költözködés vagy tatarozás esetén),
az új dolgozók oktatása,
dohányzás a számítógépes környezetben,
a levegõ páratartalma,
mûszálas anyagok alkalmazása,
EPH (egyen-potenciálra hozás), megfelelõ földelés, megbízható szünetmentes áramellátás, túlfeszültség ellen védõ berendezések, mindezek karbantartása, ellenõrzése.

- Hálózatfigyelõ programok használatával is feltárhatók különbözõ veszélyforrások (gyenge jelszavak, puffer-túlcsordulások, korlátlan FTP hozzáférés, jelszó nélkül használható szolgáltatások, nyitott TCP vagy UDP portok, a nem biztonságos szolgáltatások,…).
- A tûzfalak tájékoztatásának vizsgálatával megtudhatjuk, hogy milyen gyanús eseményeket észlelt és hogyan hárította el ezeket.
- Meg kell vizsgálni a szolgáltatásban megjelenõ adatok szükséges és elégséges mennyiségét.
- Minõsített adatok esetén az alapadatokat és biztonsági másolatokat más földrajzi helyen tárolják-e?
- Az adatok, adatállományok rejtjelezettek-e a megfelelõ rejtjelezési eljárással?
- Adathozzáférések ellenõrzése. Rögzítették-e a hozzáférési jogosultságot?
- Az adatforgalom naplózásával kapcsolatban: az adatok naplózása megfelel-e a törvényi szabályozásnak, az adatvédelemnek? Megoldott-e a naplózott anyagok tárolása?
- A betörés felderítésére leggyakrabban naplófájlokat és különbözõ betörésvédelmi rendszereket alkalmaznak, így esetleg idejében megtudhatók a betörési kísérletek vagy a megtörtént akciók.
- A felhasználói szintek ellenõrzése: kinek van rendszergazdaként joga belépni a rendszerbe, milyen csoport milyen jogosultságot használhat, a beállított felhasználói jogok vizsgálata.
- A legújabb programokat használják-e, telepítik-e a programkészítõk hibajavításait?
- A vírusirtó és trójai faló észlelõ programok ellenõrzik-e az elektronikus levelezést?
- A biztonság megteremtését segítheti a távfelügyeleti szolgáltatások igénybe vétele, ami lehetõvé teszi, hogy a számítástechnikai hálózatok egy külsõ monitoring-rendszer segítségével folyamatosan kontroll alatt álljanak. Ez a megfigyelõ rendszer rögzíti az informatikai rendszer ellen irányuló különbözõ hacker támadásokat és vírusfertõzéseket.

- Etikus információ-szerzésnek nevezhetnénk azt az internetes biztonságtechnikai szolgáltatást, amelynek segítségével, nem informatikai úton információkat próbálnak megtudni a rendszerrõl. A szimuláció során a kísérletet végzõk arra kíváncsiak, hogy a szervezet munkatársaival való beszélgetések alkalmával milyen mûszaki információkhoz lehet hozzájutni, amelyeket esetleg rossz szándékú támadó is megszerezhet.

Annak érdekében, hogy a veszélyforrás feltárása áttekinthetõ legyen, célszerû különbözõ csoportosításokat, táblázatokat használni.

A VESZÉLYFORRÁSOK CSOPORTOSÍTÁSA								
infrastruktúra	hardver	szoftver	adathordozók	dokumentumok	adatok	kommunikáció	személyek	egyéb

3.2. A kockázatelemzés folyamata

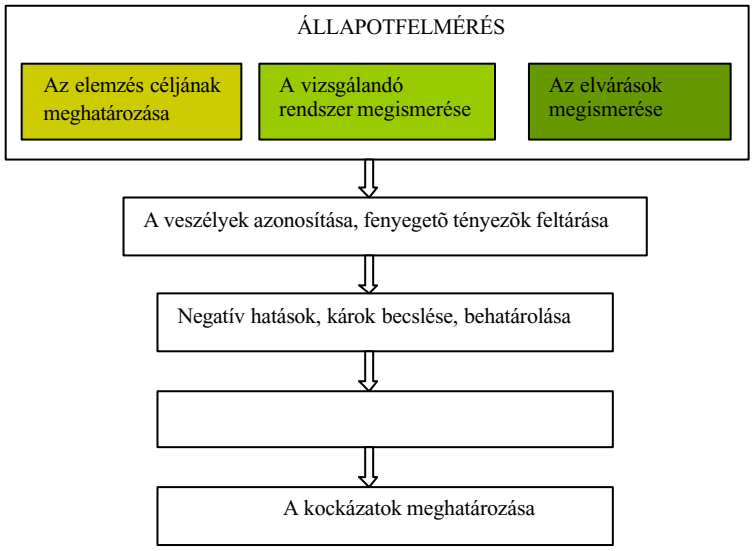
A fejezetben a kockázatelemzés folyamatának részletes leírásával foglalkozom. Az egyes lépések után a védelmi szféra egy szegmensére vonatkozó, nem teljes körû gyakorlati megvalósíthatóság szerepel.

A kockázatelemzés elvégzését a rendelkezésemre álló szakirodalom, különösen a második fejezetben leírt elemzési módszerek tanulmányozása, összehasonlítása és a következtetések levonása után az alábbi öt lépésben tartom a legcélravezetõbbnek:

(1) ÁLLAPOTFELMÉRÉS (a cél, a rendszer és az elvárások megismerése)
(2) A VESZÉLYEK AZONOSÍTÁSA, FENYEGETÕ TÉNYEZÕK FELTÁRÁSA
(3) NEGATÍV HATÁSOK, KÁROK BECSLÉSE, BEHATÁROLÁSA
(4) A KÁROK GYAKORISÁGÁNAK MEGHATÁROZÁSA
(5) A KOCKÁZATOK MEGHATÁROZÁSA

Az öt lépéses módszertan elõnyeit a jó áttekinthetõségben, a gyakorlati megvalósíthatóságban látom. Eddigi tapasztalataim szerint a módszer kellõen tagolt, áttekinthetõ, egyben biztosítja a szükséges részletességet és alkalmas a védelmi szféra informatikai rendszereinek vizsgálatára.

3.2.1. A kockázatelemzés közvetlen céljának, a vizsgálandó rendszernek a meghatározása, az elvárások megismerése



Az elemzés céljának meghatározása:
A következõ kérdésekre kell választ kapnunk:
- Milyen indokok tették szükségessé a kockázatelemzést?
- Ha az indokok között felállítható valamilyen fontossági sorrend, mi ez a sorrend?

3.3. ábra. A módszertani útmutató lépései; állapotfelmérés

A kapott válaszokból meg kell határozni:
- a kockázatelemzés fõbb célkitûzéseit,
- az informatikai rendszer sikeres mûködésének feltételeit,
- a rendszer meghibásodásának feltételeit.

A vizsgálandó rendszer meghatározása: (helyzetfeltárás, követelmények, problémák, korlátok és a rendszer céljainak, feladatainak azonosítása)

Ismernünk kell:
- a rendszert általánosan,
- a rendszer környezetét,
- a vizsgálandó rendszerrel fizikai kapcsolatban lévõ minden más rendszert, a kapcsolódási pontokat, a határokat,
- a vizsgálandó rendszerrel funkcionális kapcsolatban lévõ minden más rendszert, a kapcsolódási pontokat, a határokat,
- a rendszerhatárokon áthaladó információk típusait, az áramlás irányát, (Ha az adatfolyam ábrákon - Data Flow Diagram, DFD - együtt ábrázoljuk a rendszer folyamatait és adatait valamint elkészítjük a kapcsolódó leírásokat is, akkor az adott információs rendszerrõl átfogó képet kapunk.)
- a rendszer külsõ objektumait,
- az egyes tevékenységeket alrendszerenként,
- adatkezelést, az adatok átadásának ill. átvételének nyugtázását, az adathordozók és adatok tárolási biztonságát, az adathordozók és adatok hozzáférési jogosultsági rendszerét, az adathordozók és adatok megsemmisítését, az adathordozók közötti adatmásolást,

- adatkezelés célhoz kötöttségét,
- az adatok minõségét,
- az adattovábbítást, az adatkezelések összekapcsolását,
- az érintettek jogait és érvényesítésüket,
- az informatikai rendszer alkalmazásait,
- azokat a szabványokat, jogszabályokat, helyi rendeleteket, amelyek az informatikai rendszer mûködésével kapcsolatosak,
- a számítástechnikai eszközök mûszaki és erkölcsi állapotát, karbantartását, nyilvántartását, tárolását, tûz és vagyonvédelmi biztonságát, üzembiztonságát, árnyékolás jellegû védelmét,
- a szoftverek erkölcsi állapotát, karbantartását, nyilvántartását, tárolását, vírusvédelmet, tûzfal rendszert, hozzáférési jogosultságok[25] rendszerét és kezelését,
- az informatikai rendszer kezelõinek, használóinak felkészültségét,
- a katasztrófa-tervet, a minimális mûködési tervet, a teljes rendszer-visszaállítás tervét.

Az elvárások megismerése:

Az elvárások megismerése a felhasználó védelmi céljainak rögzítését, az informatikai rendszer iránt támasztott igény pontos megfogalmazását jelenti. Továbbá itt kell feltárni az esetleges korábbi ellenõrzések alkalmával észlelt hiányosságokat és a foganatosított intézkedéseket.

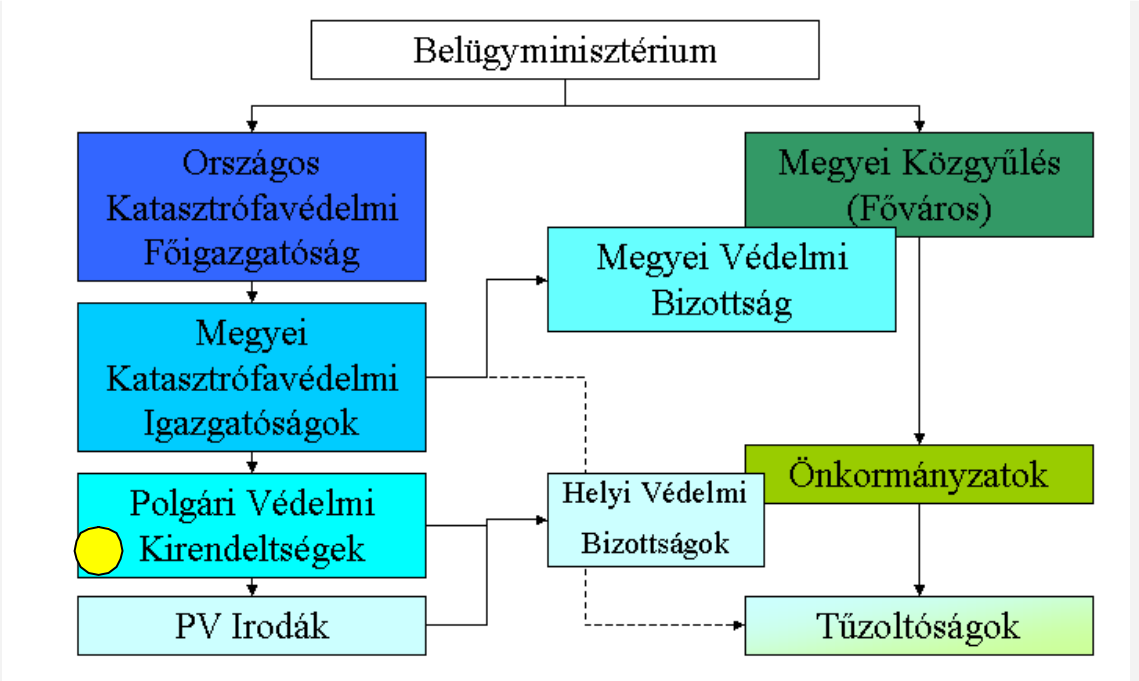
A védelmi igényeket ketté választhatjuk az információvédelem és a megbízható mûködés területére. Az információvédelem az adatok bizalmasságának, hitelességének és sértetlenségének a biztosítását jelenti. A megbízható mûködés a rendelkezésre állást, funkcionalitást foglalja magában. A szervezeteknél rájuk jellemzõ prioritási sorrend állítható fel. Például egy konfliktus kezelõ központ belsõ informatikai rendszerénél elsõdleges szempont lehet a rendelkezésre állás, de abban az esetben, ha egy nem megfelelõ idõben kijutó döntés nagy kárt okoz, úgy a bizalmasságnak lehet prioritása.

Az állapotfelmérés megvalósítása a gyakorlatban:

(A továbbiakban az egyes lépések példákon való illusztrálását a szerkesztésnél kiemelem, téglalapba helyezem és háttérszínt használok.) A Fõvárosi Polgári Védelmi Igazgatóságtól a nagyon sok segítség mellett engedélyt is kaptam ahhoz, hogy a szervezet informatikai rendszerérõl szerzett ismereteket a dolgozatomban publikáljam.

[25] MSZ ISO/IEC 17799:2002 Informatika. Az informatikai biztonság menedzselésének eljárásrendje szabvány 9. szakasza Hozzáférési jogosultság, felügyelet.

Az elõzõek figyelembevételével a védelmi szféra egy részterületének állapotfelmérése a következõképpen valósítható meg. Tehát a kiválasztott terület a **Fõvárosi Polgári Védelmi Igazgatóság**, amelynek helyét a Belügyminisztériumon belül a következõképpen lehet szemléltetni:



A polgári védelem feladata:

Az Országgyûlés által 1996-ban elfogadott XXXVII. törvény, amely a polgári védelem feladatait, rendszerét, az állampolgárok kötelezettségeit, a polgári védelem irányítási rendszerét, jog- és hatáskörét szabályozza, kimondja a 2. §. (1) alpontban, hogy a "…polgári védelem: a honvédelem rendszerében megvalósuló szervezet, feladat- és intézkedési rendszer, amelynek célja a fegyveres összeütközés, a katasztrófa és más veszélyhelyzet esetén a lakosság életének megóvása, az életben maradás feltételeinek biztosítása, valamint az állampolgárok felkészítése azok hatásainak leküzdése és a túlélés feltételeinek megteremtése érdekében…"

Ezen célok megvalósításához jól mûködõ információs rendszerre van szükség, amelynek segítségével összehangolt tevékenységek végezhetõk.

A kockázatelemzés célja:

A polgári védelemnek a feladatai ellátásához szükséges információ mennyisége folyamatosan növekszik, a nagy mennyiségû információ kezelése informatikai eszközökkel lehetséges. A nagy informatikai függõség miatt fontos az informatikai rendszerek biztonságos üzemeltetése, ami kockázatelemzéssel támogatható. Azonosítani kell azokat a biztonsági réseket, fenyegetõ tényezõket, amelyek potenciálisan nagy kárt okozhatnak a szervezet számára, így magas kockázatot jelentenek. Ennek ismeretében megvalósítható a kockázatarányos védelem, ami megfelelõ védelmi szintet jelent optimális biztonsági költségek mellett. Az elemzés az alapja a hosszú távú és megbízható tervezésnek, az informatikai rendszer elvárt szintû mûködtetéséhez,

fejlesztéséhez döntési alapot kell biztosítani, ami figyelembe veszi az elvárásokat és a lehetõségeket.

A vizsgálandó informatikai rendszer meghatározása:

A Fõvárosi Polgári Védelmi Igazgatóság informatikai rendszerének felépítése:

A helyi számítógép-hálózat a Fõpolgármesteri Hivatal 10/100 Mbit/s sebességû UTP hálózata[26], közel 300 végponttal és aktív elemekkel. A fõ rack szekrény[27] a 2. emeleten helyezkedik el, az irodák strukturált hálózaton az 1. emelet helyi rack szekrénybõl UTP kapcsolaton jutnak a 2. emeleti fõ gyûjtõbe. Az egyes szinteket illetve a HUB[28]-okat Switchek[29] kapcsolják egymáshoz.

A rendszer üzemeltetése:

Az informatikai rendszerek üzemeltetéséért a Fõvárosi Polgári Védelmi Igazgatóság Gazdasági és Mûszaki Osztály Híradó-informatikai Csoport személyi állománya a felelõs, amely kiterjed a hálózatok, szerverek valamint a kliensek felügyeletére.

A rendszer üzemeltetését segítõ egységek:

Lotus Notes Levelezõ Rendszer:

A rendszer a Mogyoródi úti épületben helyi hálózaton keresztül, míg a megyei igazgatóságok és háttérintézmények tekintetében kapcsolt telefonvonalakon, illetve ISDN 30-on[30], RAS 1500-on[31] keresztül érhetõ el. Jelenleg 1 db Lotus Notes Domino R5 szerver és 85 kliens licenc áll rendelkezésre. A Lotus Notes Levelezõ Rendszerhez a vezetõi állománynak, a titkársági osztálynak, valamint az ügyeletnek van hozzáférése.

Complex CD Jogtár: Hatályos jogszabályok, jogszabályok, közbeszerzések, közlönytár, döntvénytár, törvény indoklás, törvényjavaslatok, vámtarifák, önkormányzati normák összessége. A Fõvárosi Polgári Védelmi Igazgatóság alkalmazottai számára hálózaton keresztül bármikor elérhetõ. A jogtár üzemeltetését a Fõpolgármesteri Hivatal Informatikai Ügyosztálya végzi. Korlátlan licenc számmal rendelkeznek, így a

---

[26] UTP hálózat: **U**nshielded **T**wisted **P**air, UTP, csavart, vagy más néven sodrott érpár, két szigetelt, egymásra spirálisan felcsavart rézvezeték. Ha ezt a sodrott érpárt kívülrõl egy árnyékoló fémszövet burokkal is körbeveszik, akkor STP- rõl (Shielded Twisted Pair, árnyékolt sodrott érpár) beszélünk. A csavarás a két ér egymásra hatását küszöböli ki, jelkisugárzás nem lép fel. Általában több csavart érpárt fognak össze közös védõburkolatban. Pontosan a sodrás biztosítja, hogy a szomszédos vezeték-párok jelei ne hassanak egymásra (ne legyen interferencia).

[27] rack szekrény: amely számítástechnikai eszközök, illetve szerverek elhelyezésére jól alkalmazható, zárható, fémszekrény, a kábelbevezetésre a szükségleteknek megfelelõen van lehetõség.

[28] HUB: passzív hálózati eszköz, mely a szegmensek kapcsolatát biztosítja.

[29] Switch: kapcsoló, olyan szerkezeti elem, amely útvonalszegmensek idõleges egymáshoz rendelésével épít fel kommunikációs útvonalat.

[30] ISDN 30: 30 db alapcsatornát tartalmaz, amelyet elsõsorban nagy kommunikációigényû vállalatok alkalmaznak, mivel 30 telefonvonalat tartalmaz, amelyhez körülbelül 100 telefonszám rendelhetõ.

[31] RAS 1500: távoli hozzáférésû szerver (**R**emote-**A**ccess-**S**erver)

hálózaton keresztül a szükséges igényeket a rendszer ki tudja szolgálni. Jelenleg kb. 25 munkaállomás használja. Frissítése rendszeres idõközönként (általában havonta) történik.

Forrás SQL:
Pénzügyi integrált rendszer, mely a fõkönyvi, pénztári és a készletnyilvántartással foglalkozik. Az Igazgatóságon 4 kliens és 1 szerveralkalmazás (SQL) áll rendelkezésre. A hozzáférést a Gazdasági és Mûszaki Osztály személyi állományának teszik lehetõvé.

SZENYOR: (Személyzeti Nyilvántartó Országos Rendszere)
Feladata az alkalmazottak személyzeti jellegû adatainak nyilvántartása. Igazgatóságon 1 szerver és 1 kliens, valamint a Fõigazgatóságon 1 szerver és 10 kliens áll rendelkezésre. A hozzáférést a Személyzeti és Oktatási Osztály személyi állományának teszik lehetõvé.

ArcView METAFRAME:
A rendszer Citrix Metaframe kliensen keresztül a helyi hálózaton, illetve ISDN 30-on, RAS 1500-on keresztül érhetõ el. A rendszer jellegzetessége, hogy a programok a szerveren futnak és a térkép, valamint a hozzá kapcsolódó adatbázisok is a szerveren vannak, így a hálózaton és a telefonvonalakon csak a képernyõ kép tartalma áramlik, így a telefonvonalak viszonylag kis sávszélessége ellenére is, a rendszer távolról is hatékonyan mûködik. Jelenleg 20 megyei igazgatóság rendelkezik helyi térinformatikai munkaállomással és a szükséges kliensekkel. A Fõigazgatóság Veszélyhelyzet Kezelési Központ, a megyei igazgatóság Veszélyhelyzet Kezelési Központ, valamint a Nukleáris Biztonsági Intézkedés és Értékelõ Központ kap hozzáférési jogot. A rendszer fõvárosi végpontját a Híradó-informatikai Csoport kezeli.

ETRUST Antivírus:
Az Igazgatóságon belül valamennyi felhasználó gépére fel van telepítve, amely a hálózaton lévõ gépeket védi a vírustámadás ellen. A legújabb antivírus-frissítések letöltésével naprakész felügyeletet biztosít a felhasználók részére.

Nyomtatószerver:
Jogosultságtól függõen, a hálózaton keresztül hozzáférést biztosítanak a nyomtatókhoz a felhasználóknak.

Fileszerver:
Jogosultságtól függõen a felhasználók a hálózaton keresztül hozzáférhetnek különbözõ alkalmazásokhoz és dokumentumokhoz. Az ISO folyamatleírás dokumentumaihoz

valamennyi felhasználónak hozzáférést biztosítanak. (Server „K” meghajtó „ISO” könyvtárában)

Katasztrófavédelem rádiórendszere:
A fõvárosi katasztrófavédelem rádiórendszerének üzemeltetéséért a Híradó-informatikai Csoport személyi állománya a felelõs, ami kiterjed a rádiórendszerrel kapcsolatos szabályzók kidolgozására, az üzemeltetés feladatára, a Belügyminisztérium illetékes szerveivel, valamint a Fõigazgatóság Távközlési és Informatikai Fõosztály szakembereivel történõ együttmûködésre.

Katasztrófavédelem távbeszélõ hálózata:
A fõvárosi katasztrófavédelem távbeszélõ hálózatának üzemeltetéséért, üzembiztonságáért a Híradó-informatikai Csoport személyi állománya a felelõs. A felelõsség kiterjed a belsõ mellékek kiosztásával, a hívás jogosultsági kategória beállításával, az üzemképes végkészülékek biztosításával, a bejövõ fõvonalak biztosításával, a telefonközpont készülékek üzemképességének fenntartásával, a szükséges bõvítések, eszköz megrendelések, javítási és karbantartási feladatok végrehajtására.

Karbantartás:
Az informatikai eszközök hardver és szoftver karbantartásáért a Híradó-informatikai Csoport személyi állománya a felelõs. Ez a felhasználói programokkal kapcsolatos problémák megelõzését jelenti; (HDD defragmentálás[32], víruskeresés, hálózati visszajelzés tesztelése, nyomtatók idõnkénti karbantartása). A fõvárosi katasztrófavédelem rádiórendszere és távbeszélõ hálózata karbantartásának szervezéséért és irányításáért a Híradó-informatikai Csoport személyi állománya felelõs. A karbantartás végrehajtást érvényes, átalánydíjas szerzõdéssel rendelkezõ cég végzi.

Felújítás, fejlesztés:
Az informatikai eszközök hardver és szoftver fejlesztéséért a Híradó-informatikai Csoport személyi állománya felelõs. Ez napi szinten az új hardver eszközök telepítését (nyomtatók, monitorok, scannerek, személyi számítógépek) jelenti a rövid- és középtávú jóváhagyott fejlesztési tervek alapján.
A fõvárosi katasztrófavédelem rádiórendszere és távbeszélõ hálózata felújításának és fejlesztésének szervezéséért és irányításáért a Híradó-informatikai Csoport személyi állománya felelõs. A távbeszélõ hálózat bõvítését, fejlesztését, felújítását, árajánlatkérést követõen a nyertes céggel vállalkozási szerzõdés alapján végeztetik el.

[32] defragmentálás =töredezettség-mentesítés

Javítás:

Munkaidõben folyamatos a rendelkezésre állás. A Fõpolgármesteri Hivatal Informatikai Ügyosztálya komolyabb problémákra 24 órás ügyeletet üzemeltet. A szerverekrõl heti, illetve havi archiválás történik. Tervszerû, megelõzõ intézkedéseket kell végrehajtani az esetleges váratlan problémák elhárítása érdekében. Ennek részeleme a készletgazdálkodás, mely az alábbi eszközökre terjed ki: RAM, HDD, videó-vezérlõ, hálózati kártya, floppy, CD-ROM, egér, klaviatúra stb.

A katasztrófavédelem rádiórendszere folyamatos üzemének biztosítása érdekében a hibabejelentések fogadására 24 órás szolgálat áll rendelkezésre. A hibabejelentés Hibabejelentõ lapon történik, mely tartalmazza a hibás berendezés, a bejelentõ adatait és a bejelentés idõpontját. A hibabejelentés alapján a vállalkozó árajánlatot ad a javítás elvégzésére. A munkálatok elvégzését ezután rendelik meg. Az elvégzett munka igazolása a Híradó-informatikai Csoport vezetõje által aláírt munkalappal történik.

A távbeszélõ hálózat és elemeinek javítását a Híradó-informatikai Csoport biztosítja. Az igénylõ hibabejelentését követõen kerül megrendelésre a hiba jellegétõl függõen a helyszíni vagy a szakszerviz általi javítás.

Elvárások megismerése:

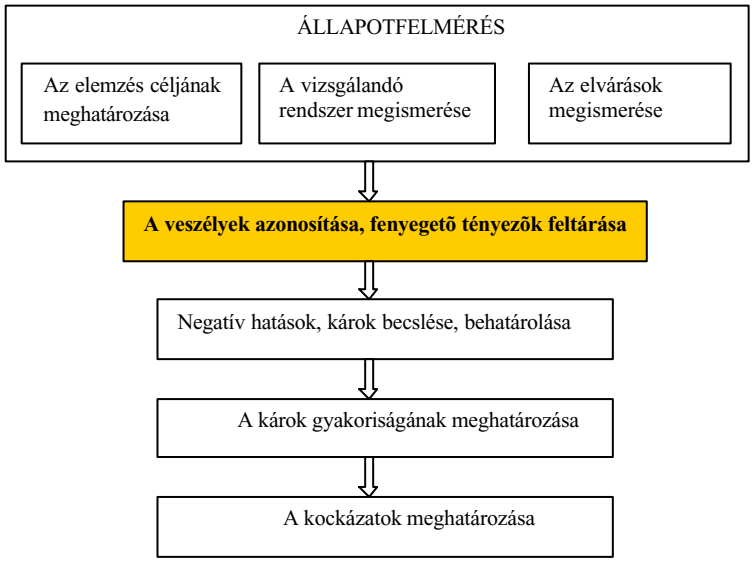
Az elvárások megismeréséhez feltérképeztem a védendõ erõforrásokat, amelyek megfelelõ mûködése elengedhetetlen ahhoz, hogy a vizsgált informatikai rendszer az elvárásokat biztosítani tudja:

1.	Infrastruktúra 1.	A 2. emeleti fõ rack szekrény és szerver szoba
2.	Infrastruktúra 2.	Az 1. emeleti helyi rack szekrény és szoba
3.	Infrastruktúra 3.	Az épületrész, ahol az adott informatikai rendszer mûködik.
4.	Kapcsolt telefonvonalak	A Lotus Notes Levelezõ Rendszert a FPVI kapcsolt telefonvonalakon éri el.
5.	Kommunikációs vonalak	Bérelt vonali 128 kbit/s kapcsolat Cisco Router-en 1db BM Intranet
6.	Adatbázisok	Személyügyi (Szenyor), Karrierfejlesztési (Peodesy), (Peodesy-kompetencia vizsgáló szoftver) Pénzügyi- számviteli programrendszer (Forrás SQL), pénztár, fõkönyv, készlet, -modulok Kommunikációs (Calisto) Levelezõ Lotus Notes Minõségbiztosítási rendszer (ISO9002)

		Megjegyzés: A felmérés 2003.10.7-én készült. Az ISO 9002 szerinti tanúsítás 2003. decemberében lejár, érdemes áttérni az ISO 9001:2000 minõségirányítási rendszerre.
7.	Adatok	Személyügyi –saját személyügyi szerveren (NT) Pénzügyi-számviteli – távoli szerveren, védett adatátviteli úttal Calisto -távoli szerveren- védett Lotus Notes -saját Novell Szerveren napi mentéssel +távoli szerveren replikázva ISO -saját Novell Szerveren csak olvasható
8.	Dokumentumok	72000 db, elhelyezés munkaállomáson, másolatok, CD-n, mágneslemezen, Novell file szerveren
9.	Számítógépek	35 db munkaállomás irodákban, 4 db szerver, szerverszobában elzárva, klíma, Raid-5, elhelyezés
10.	Egyéb hardver	1 db Zip drive, 1 db DAT drive (szalagos) szerverekben, 6 db CD író archiválásra gépekben
11.	Programok	30 db-os Microsoft CD software készlet Irodai 4 db +Szakmai alkalmazások 6 db +Vírusvédõ kétféle 4-4 csomag
12.	Adathordozók	3750 db mágneslemez, (874 db CD-800MB/db), 15 db ZIP (250MB) lemez, 12 db (GB) DAT kazetta

3.2.2. A veszélyek azonosítása, fenyegetõ tényezõk feltárása

Az informatikai biztonság alapja a bizalmasság, a sértetlenség, a rendelkezésre állás, a hitelesség, a mûködõképesség. A veszélyforrások ennek az öt alaptényezõnek a sérülését okozhatják.



3.4. ábra. A módszertani útmutató lépései; a veszélyek azonosítása, fenyegetõ tényezõk feltárása

Ebben a szakaszban kell meghatározni az informatikai rendszer gyenge pontjait, és azokat a fenyegetõ tényezõket, amelyek a védendõ informatikai alkalmazásokra, adatcsoportokra közvetlenül vagy közvetve veszélyesek lehetnek.

A fenyegetõ tényezõk sokfélesége miatt célszerû valamilyen csoportosítást alkalmazni, de az egyes csoportok hatása összeadódhat, erõsítheti egymást, tehát nem lehet az egyes csoportok hatását mechanikusan külön-külön figyelembe venni.

Humán tényezõk:

A humán veszélyforrás azt jelenti, hogy a hiba, a káresemény emberi tevékenység következményeként lép fel.

Az angol nyelvû szakirodalomban „7-E” néven találkozunk az informatikai biztonságot fenyegetõ legfontosabb humán tényezõkkel.

Ego -személyiség, hiúság **E**avesdropping - elektronikus lehallgatás

Enmity –ellenségeskedés **E**spionage -kémkedés

Embezzlement –sikkasztás **E**xtortion –zsarolás **E**rror –hibás döntés

A hét tényezõ mindegyike az emberhez kapcsolódik, így az informatikai biztonság hatékonyságát nagymértékben növelheti az emberi oldalra történõ odafigyelés.

Az ember által okozott károkat célszerû két csoportra osztani:

Nem szándékos károkozás, aminek az okai nagyon szerteágazóak, de a leggyakrabban elõfordulók a következõk lehetnek;

gondatlanság,

személyes vagy munkahelyi problémák miatt kialakult figyelmetlenség,

szabványok, belsõ elõírások, szabályok ismeretének hiánya,

képzetlenség, alkalmatlanság, hozzá nem értés,
a belsõ elõírások, munkaköri leírások figyelmen kívül hagyása,
nem megfelelõ elõírások, szabályok, rosszul szabályozott munkafolyamat,
a valós veszélyek fel nem ismerése, felelõtlenség,
a túl bonyolult munka vagy túl egyhangú munka miatti tévesztések,
hibás munkavégzés, hanyagság, az elõírások megszegése kényelmi okokból, az ellenõrzések hiánya.
Egy szervezetben veszélyforrás a változás is, pl. személyi változás, struktúraváltozás.

Tudatos károkozás: az említett „7-E”-bõl hat ezzel az esettel foglalkozik.

A kockázatelemzés során a vizsgált szervezet minden egyes munkakörét ellenõrizni kell veszélyeztetettség szerint. Az egyes munkakörökben veszélyforrás lehet az alkoholizmus, a drogfüggõség, a játékszenvedély, a zsarolhatóság.

Az informatikai biztonságot vizsgáló cégek statisztikái szerint a betörések 80%-át a szervezetek saját alkalmazottai követik el. A sértõdött vagy elbocsátott emberek, a rendszer-ismeretükkel nagy károkat okozhatnak.

Az okok általában; irigység, sértettség, bosszú, vandál pusztítási vágy, rosszindulat, hirtelen felindulás, hírszerzés és ipari kémkedés támogatása, információszerzés anyagi vagy egyéb elõnyökért.

Potenciális veszélyforrás a versenytársak agresszív érdekérvényesítése; beépített emberek, új állással kecsegtetett, titkos adatokat kiadó kutatók, lefizetett kisegítõ személyzet információi segíthetnek egyes cégeket a konkurenciával szembeni versenyben.

Az Amerikai Védelmi Minisztérium skálája szerint, a nem katonai alkalmazásoknál a legmagasabb minõségi fokozattal minõsített rendszerek biztonságos mûködésének szinte egyetlen veszélyforrása van, a személyzet.

Nem a technológia, hanem emberi mulasztás okozza az informatikai rendszerek biztonsági hiányosságait, állapította meg a Számítástechnikai Ipari Szövetség (CompTIA) biztonsági felmérése. A vizsgálat arra a megállapításra jutott, hogy az informatikusok alaposabb képzése önmagában segít a védelemben[33]. Ha ilyen nagy az emberi tényezõ, mint veszélyforrás, felvetõdik a kérdés, mit lehet tenni, meg lehet valakiben bízni. A rendszergazdákban meg kell bízni, hiszen valakinek mûködtetnie kell a rendszereket, ellenõrizni a hozzáférést, védelmet nyújtani az informatikai infrastruktúra érzékeny belsõ szervei számára. A biztonságot a részrendszerekre való osztással, és egy-egy részrendszerért felelõsök kijelölésével lehet növelni.

[33] A jelentés összefoglalója http://www.bs7799.hu/comptia.pdf címen olvasható.

Logikai tényezõk, amelyek veszélyeztetik a bizalmasságot, a sértetlenséget, a rendelkezésre állást;

- az informatikai rendszerbe történõ jogosulatlan belépés, információk vagy programok jogosulatlan módosítása, rombolása, felhasználása,
- a feladó és címzett azonosítása,
- a felhasználó szerverének, címének azonosítása,
- a rendszer mûködésének megzavarása; információ lehallgatás, adatváltoztatás, adatátirányítás, adatfogadás megtagadása,
- vírus, féreg, trójai programok, logikai bomba rendszerbe juttatása, (A számítógépes vírusok által okozott károk nagyok lehetnek és növekvõ tendenciát mutatnak.)
- karbantartási és fejlesztési tevékenységek során elkövetett biztonsági és egyéb hibák. Ha az intézmények nem körültekintõen leinformált külsõ céget bíznak meg a hardver- és a szoftverkarbantartással, archiválással, auditálással ez a veszély fokozódik.

A leggyakoribb veszélyforrások:

Nagyobb a veszély, ha a rendszert nem egy szûk csoport használja, hanem egyik oldalról *nyitott a rendszer* például az ügyfelek, külsõ felhasználók számára. Az *otthoni munka*, amely során a dolgozók részben vagy egészben otthon végzik el feladataikat, fokozhatja a veszélyeket.

Az informatikai eszközök mûködésben levõ hardverei körül elektromágneses mezõ van, az elektromágneses sugárzás érzékeny vevõkészülékekkel felfogható és dekódolható. Ha a számítógépterem *árnyékolatlan vagy nem folytonos az árnyékolás*, akkor lehallgathatóság, a kívülrõl megzavarható adatbázis és a rendszer károsodása vagy légköri zavarok fenyegetik a rendszert. Ha *a kommunikációs hálózat* (pl. telefonvonal) *lehallgatható*, úgy az informatikai rendszer teljesen kiszolgáltatott a támadásoknak.

A *jelszavak*kal kapcsolatban; a nem megfelelõ, túl könnyû, más biztonsági módszerekkel nem kombinált jelszó, ha a használatban emberi hibák sokasága lép fel (hanyagság, a jelszó jegyzetfüzetbe írása vagy más személynek való kiadása), ha lehallgatható vagy titkosítatlanul tárolt a rendszerben, ha a jelszavak valamilyen módszerrel kilistáztathatók, ha nem történik változtatás megfelelõ idõközönként, ha egy jelszót többen is használnak.

A *naplózás* is egy veszélyforrás, a napló tartalmát is védeni kell.

A *rejtjelezésbõl adódó problémák*; olyan algoritmus alkalmazása, amit már feltörtek vagy életciklusa utolsó szakaszában van. A rejtjelezõ algoritmusok általában jól kidolgozottak, a nagyobb veszélyt a kulcsok kiosztása vagy tárolása vagy a rövid kulcs jelenti. Fenyegetõ tényezõ, ha valamilyen szöveg nyílt formában és rejtjelezett formában is megvan a rendszerben.

Fizikai tényezõk:

A jogosulatlan hozzáférés, mint veszélyforrás két részre bontható. A külsõ támadás, amikor a támadók célja az informatikai eszközök megszerzése vagy tönkretétele. A

belsõ támadás, ha a szervezet dolgozói az informatikai eszközöket, szolgáltatásokat jogosulatlanul használják.
Az eszközök rendelkezésre állása sérül, ha az épület, ahol az informatikai eszközök vannak, fizikai védelme nem megfelelõ; ajtók, ablakok, tûzfalak, vezetékek, elektromos és távbeszélõ eszközök elhelyezése nem szabványszerû és nem az elõírt minõségû, vagy ha az épületben mûködési zavar lép fel, mint például az áramellátó- vagy biztonsági rendszerek meghibásodása.

Környezeti tényezõk:
- Magyarországon az egyik leggyakoribb környezeti veszélyforrás a villámcsapás illetve a villámcsapásból eredõ másodlagos túlfeszültség.
- Az árvíz és belvíz elsõsorban az épületekben tesz kárt és így fokozza a veszélyt. Árvizek 809 települést kiemelten veszélyeztetnek Magyarországon.
- A földrengések, tûzhányó-kitörések nálunk nem, de más országokban számottevõ veszélyforrást jelenthetnek.
- Egyéb pusztító katasztrófák; tûzvész, szélvihar. Ilyen szempontból Magyarország közepesen katasztrófaveszélyes területnek számít.
- Mûszaki zavarok, amelyek különbözõ súlyosságú és idõtartamú kiesést idézhetnek elõ informatikai rendszerben és szolgáltatásban.
- Nedvesség (csõrepedés, billentyûzetre ömlõ folyadék, páralecsapódás, nagy páratartalom), napsütés, szélsõséges hõmérsékletingadozás, por, füst (dohányzás), agresszív gõzök, túlzott jármûforgalom.
- Elektromos kisülések, elektromos hálózat zavarai (feszültség letörés, feszültség túllövés, tranziens csúcsok, feszültség kimaradás, hálózati zaj, feszültség torzulás, frekvencia változás, felharmonikusok), statikus elektromosság.
- Mechanikai sérülések, rágcsálók, ízeltlábúak (vezetékek átrágása, érintkezési zavarok, zárlat).

A fenyegetõ tényezõknél figyelembe kell venni az egyes védelmi intézkedések járulékos hatását is. Egy rendszerelemre vonatkozóan elsõdlegesen alkalmazott intézkedések más rendszerelemekre ható gyengítõ vagy erõsítõ hatását a szakirodalom szinergikus hatásnak nevezi. Egyenszilárdságú védelmi rendszer úgy alakítható ki, ha a szinergikus hatásokat is vizsgáljuk és úgy kompenzáljuk, hogy a kockázattal arányos védelmi szint minden rendszerelemre megvalósuljon. A szinergikus hatások mértékének megállapításához a gyakorlatban matematikai statisztikai módszerek alkalmazása és megfelelõ tapasztalat szükséges.

A vizsgált rendszert módszeresen át kell vizsgálni abból a célból, hogy a jelenlevõ, de még problémát nem okozott veszélyeket azonosítsuk. Különbözõ veszélyazonosító módszereket ismerünk, amelyeket három fõ csoportba sorolhatunk;
- összehasonlító módszerek,

- fundamentális módszerek,
- induktív elemzõ módszerek.

Az *összehasonlító módszerek* olyan veszélyelemzési módszerek, amelyek felsorolásszerûen megadják vagy rangsorolják azokat a veszélyeket, veszélyforrásokat, amelyeket elemezni szükséges.

A *fundamentális módszerek* strukturált eljárások, amelyek segítségével megvizsgálják a rendszer részeit, és a „mi van, ha ez vagy az történik, nem történik" típusú kérdésekre keresik a választ.

Az *induktív elemzõ módszerek*, amelyekkel sokféle kezdeti eseménybõl következtetnek a végsõ eseményekre.

A fenyegetõ tényezõk feltárásának gyakorlati megvalósítása:

A fenyegetõ tényezõk feltárása a példaként felhozott szervezetnél részleges; a teljes körû, minden rendszerelemre vonatkozó gyengepont-elemzés és ennek nyilvánosságra hozása önmagában is veszélyforrás.

Infrastruktúrával kapcsolatos veszélyforrások:

- A Fõvárosi Polgári Védelmi Igazgatóság nem különálló épületben, hanem a Fõpolgármesteri Hivatal jól elkülönített részében van. A Fõpolgármesteri Hivatalban 24 órás portaügyelet, a FPVI-on 24 órás ügyeleti szolgálat van. A Fõpolgármesteri Hivatalban munkaidõben ügyfélfogadás van, így gyakorlatilag a FPVI épületrészébe illetéktelenek is könnyen bejuthatnak. *Beléptetõ rendszer nincs.*
- Az *Informatikai Biztonsági Szabályzat kidolgozása folyamatban van*, de ennek hiányában a vonatkozó elõírások betartatása és ellenõrzése csak részben megoldott.
- *Szerviz szerzõdés* a BM tulajdonú eszközökre van, az *FPVI eszközeire nincs*.

Hardverrel kapcsolatos veszélyforrások:

- A gépek 27%-a elavult, a fejlesztés lassú.
- A mentések, az archivált anyagok zárt helyiségben, lemezszekrényben elzárva, természeti hatásoktól részben védett helyen vannak tárolva.
- A mûszálas anyagok elektromos kisüléseket okozhatnak, ezt a tényt a szerverszobában figyelembe veszik, a többi helyiségben részben.
- Egységes hardvermárkák kialakítása és a biztonsági tartalékok képzése nem megoldott.

Szoftverrel kapcsolatos veszélyforrások:

- A szoftverellátás központi, de hiányos.
- A különbözõ szoftverek részben összehangoltak.
- Elõfordulhat házilag gyártott, nem megfelelõen tesztelt szoftver.

Adathordozókkal kapcsolatos veszélyforrások:

- Külsõ adathordozók, lemezek kerülhetnek a számítógépekbe.

Dokumentumokkal kapcsolatos veszélyforrások:

- Új iratkezelési szabályzat van kiadás alatt.

Adatokkal kapcsolatos veszélyforrások:

- Adathordozók által okozott adatvesztések.
- Emberi szándékos vagy akaratlan törlések.

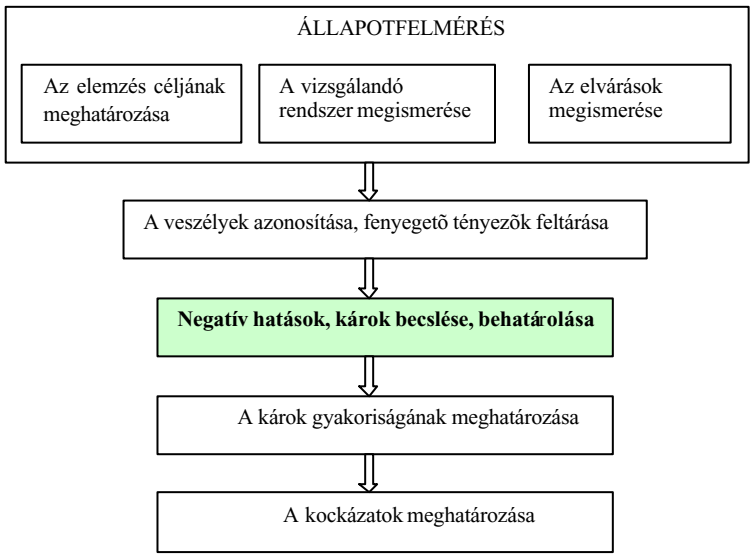
Kommunikációval kapcsolatos veszélyforrások:

- A belsõ hálózat zárt, a külsõ hálózat részben zárt bérelt vonal, magas szintû titkosítással. Alárendeltek felé a biztonság még nem valósult meg, nyilvános internet, nyilvános távbeszélõ vonalak, modem, faxmodem, fax. Ahol van, ott BM zárt távbeszélõ hálózatának felhasználásával történik a kommunikáció.
- A Belügyminisztérium által irányított rendvédelmi szervek jelenleg használatos rádiórendszerei már kevéssé képesek lépést tartani a korszerûbb technikai eljárások alapján üzemeltett rendszerek szolgáltatásaival, forrás, fejlesztési lehetõségek hiánya, illetve a meg nem valósult kormányzati TETRA rendszer miatt.
- A kommunikációs rendszerek szélsõséges válsághelyzetekben (földrengés, ipari katasztrófa, alacsony intenzitású lokális fegyveres cselekmények stb.) nem felelnek meg a velük szemben támasztott követelményeknek. A szervezetek külön-külön mûködõ rádiórendszerei egyenként elavultak, a fejlesztések elmaradása és a központi egységes rendszer meg nem valósulása miatt. Ezek a rendszerek az elavultságuk mellett teljességgel átjárhatatlanok. Kommunikációs együttmûködés nem megoldható a szervezetek között. Az átviteli csatornák száma, minõsége, adatátviteli képessége, nagyságrendekkel marad el az ilyen helyzetekben felmerülõ igényektõl.

Személyekkel kapcsolatos veszélyforrások:

- Képzettség, informatikai ismeretek hiánya, illetve a korszerû megoldások iránti igénytelenség.
- Gyakori munkahely-változtatás, magas fluktuáció, gyakori átszervezések, leépítések, szervezeti módosítások.
- Sértettség, rosszindulat.

3.2.3. A negatív hatások, károk súlyosságának becslése, behatárolása



3.5. ábra. A módszertani útmutató lépései;
negatív hatások, károk becslése, behatárolása

- Nagyon egyszerûsített formában, biztosítási szemlélettel egyszerûen pénzösszeggel is megadhatjuk a kár súlyosságát. A probléma az, hogy nehéz megválaszolni, hogy mennyit érnek egy szervezet adatai. Elsõ megközelítésként mondhatnánk azt, amennyibe a káresemény utáni, az eredeti állapotnak megfelelõ teljes visszaállítás kerül.

Ennek a megközelítési módnak számos hátránya van, például mennyire háríthatók el a bekövetkezett károk. Általában nem lehet csak pénzösszeggel jellemezni a sebezhetõséget, az értékelésnél többféle esemény hatását is számba kell venni.

- A kár súlyosságának meghatározásánál fogalmak is használhatók, mint elhanyagolható, csekély, kritikus, katasztrofális. A gyakorlatban célravezetõ táblázatba foglalni a kategóriákat, azután emberi sérüléssel és meghatározott forint-összeggel magyarázni. Pl. a kár súlyossága más fogalmakkal, hatos szinttel az alábbi táblázat[34] szerint is lehetséges:

A kár súlyosságának meghatározása		
elnevezés	**jelölés**	**magyarázat**
elhanyagolható	eh	Az anyagi kár ≤100.000 Ft
kicsi	ki	Az anyagi kár ≤ 1.000.000 Ft
közepes	kö	Könnyû emberi sérülés, az anyagi kár ≤10.000.000Ft
nagy	n	Súlyos emberi sérülés, az anyagi kár > 10.000.000Ft
nagyon nagy	nn	Halált okozó sérülés, a szervezet mûködését rövidebb idõre megszakító esemény kárértéke.
katasztrofális	k	Tömeges sérülések, a szervezet mûködését hosszabb idõre vagy teljesen megszakító esemény kárértéke.

[34] A táblázat készítéséhez felhasználtam a BME, Hornák Zoltán, Számítógépes biztonságtechnika óravázlatát a Számítógéprendszerek analízise c. tárgyhoz

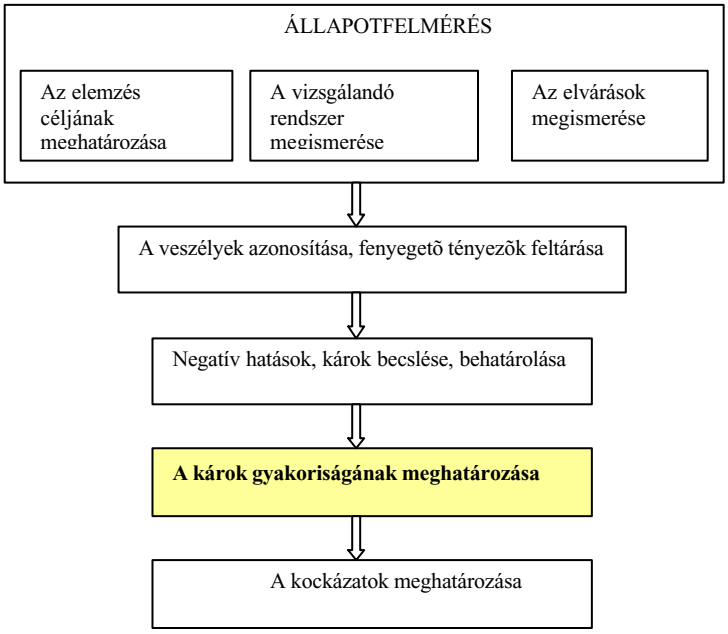
- A károk súlyosságának meghatározásánál elõfordulhat, hogy presztízs veszteséggel is számolni kell. Ismétlõdõ negatív események nem lineárisan növekvõ hanem robbanásszerû károkat is okozhatnak egy szervezet jó hírében.

A kár súlyosságának meghatározása a gyakorlatban:

A lehetséges károk súlyosságának meghatározásához a szervezet vagyontárgyainak, elemeinek értékére vonatkozó adatok és egyes események következményének ismerete szükséges.

Veszélyforrások	**A veszélyforrás jelölése**	**Kár súlyossága**
Beléptetõ rendszer hiánya	I_1	kö
Informatikai Biztonsági Szabályzat hiánya	I_2	eh
Nem teljes körû szerviz szerzõdés	I_3	eh
Lassú fejlesztés, elavult gépek	H_1	nn
Az archivált anyagok természeti hatásoktól való nem teljes védelme	H_2	eh
Mûszálas anyagok hardver közelben	H_3	eh
Nem egységes hardver márkák és a biztonsági tartalékok hiánya	H_4	ki
Hiányos szoftver ellátás	S_1	ki
A különbözõ szoftverek részben összehangoltak	S_2	eh
Elõfordulhat házilag gyártott, nem megfelelõen tesztelt szoftver	S_3	eh
Külsõ adathordozók kerülhetnek a számítógépekbe	Ah_1	n
Új iratkezelési szabályzat van kiadás alatt, az átmenettel kapcsolatos veszélyek	D_1	eh
Adathordozók által okozott adatvesztések	A_1	ki
Emberi szándékos vagy akaratlan törlések	A_2	ki
Kommunikációval kapcsolatos veszélyforrások	K_1	nn
Képzettség, informatika ismeretek hiánya, illetve a korszerû megoldások iránti igénytelenség	S_1	n
Gyakori munkahely változtatás, magas fluktuáció, gyakori átszervezések, leépítések, szervezeti módosítások	S_2	kö
Sértettség, rosszindulat	S_3	eh

3.2.4. A károk gyakoriságának meghatározása



3.6. ábra. A módszertani útmutató lépései;
a károk gyakoriságának meghatározása

A következõ kérdéseket kell általában megvizsgálni:

- a veszély fennállásának gyakorisága és idõtartama,
- a szolgáltatások meghibásodásának kiesése,
- a biztonsági készülékek meghibásodásai,
- kiszolgáltatottság a természeti elemeknek,
- személyek nem megfelelõ biztonságú tevékenységei (véletlen hibák vagy az eljárások szándékos megsértései).

Meg kell határozni az elõfordulási valószínûségek kategóriáit, például lehetnek a valószínûség kategóriái; gyakori, valószínû, eseti, ritka, nem valószínû. Itt is használhatók más fogalmak is, sõt konkrét valószínûségi értékeket (p_i) is meghatározhatunk:

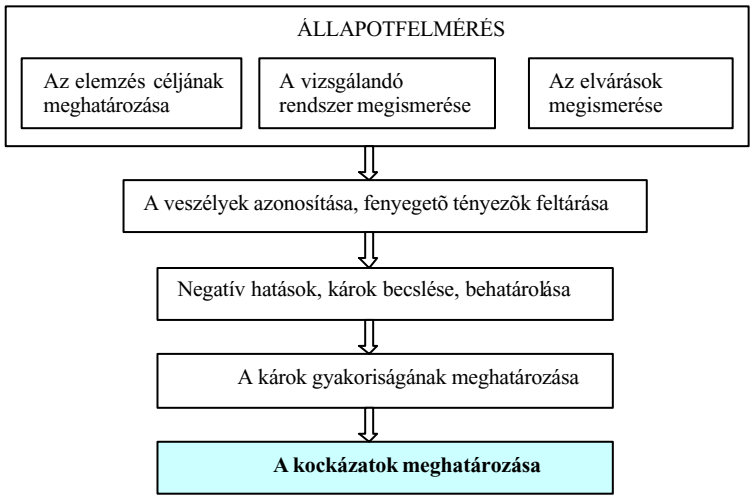
Bekövetkezési valószínûség			
elnevezés	**jelölés**	**magyarázat**	**valószínûség**
nagyon kicsi	nk	Ritkán elõforduló esemény	p_1
kicsi	k	Ötévenként elõforduló esemény	p_2
nagy	n	Évente egyszer elõforduló esemény	p_3
nagyon nagy	nn	Évente többször elõforduló esemény	p_4

A károk gyakoriságának meghatározása a gyakorlatban:

Veszélyforrások	**A veszélyforrás jelölése**	**A károk gyakorisága**
Beléptetõ rendszer hiánya	I_1	n
Informatikai Biztonsági Szabályzat hiánya	I_2	k
Nem teljes körû szerviz szerzõdés	I_3	k
Lassú fejlesztés, elavult gépek	H_1	nn
Az archivált anyagok természeti hatásoktól való nem teljes védelme	H_2	nk
Mûszálas anyagok hardver közelben	H_3	nk

Nem egységes hardver márkák és a biztonsági tartalékok hiánya	H_4	n
Hiányos szoftver ellátás	S_1	n
A különbözõ szoftverek részben összehangoltak	S_2	k
Elõfordulhat házilag gyártott, nem megfelelõen tesztelt szoftver	S_3	nk
Külsõ adathordozók kerülhetnek a számítógépekbe	Ah_1	nn
Új iratkezelési szabályzat van kiadás alatt, az átmenettel kapcsolatos veszélyek	D_1	nk
adathordozók által okozott adatvesztések	A_1	nk
emberi szándékos vagy akaratlan törlések	A_2	k
Kommunikációval kapcsolatos veszélyforrások	K_1	nn
Képzettség, informatika ismeretek hiánya, illetve a korszerû megoldások iránti igénytelenség	S_1	n
Gyakori munkahely változtatás, magas fluktuáció, gyakori átszervezések, leépítések, szervezeti módosítások	S_2	n
Sértettség, rosszindulat	S_3	nk

3.2.5. A kockázatok meghatározása



3.7. ábra. A módszertani útmutató lépései; a kockázatok meghatározása

A kockázatokat aszerint osztályozzuk, hogy a becslés szerint mennyi a valószínûsége és a potenciális súlyossága az általuk okozott bajnak, például az elõzõ táblázatok kategóriáit felhasználva, a következõ 4x6-os mátrixot definiálhatjuk.

KOCKÁZAT						
kár / valószínûség	eh (elhanyagolható)	ki (kicsi)	kö (közepes)	n (nagy)	nn (nagyon nagy)	k (katasztrofális)
nk (nagyon kicsi)	nagyon kicsi	nagyon kicsi	kicsi	közepes	nagy	**nagyon nagy**
k (kicsi)	nagyon kicsi	kicsi	közepes	nagy	**nagyon nagy**	**nagyon nagy**
n (nagy)	nagyon kicsi	kicsi	közepes	nagy	**nagyon nagy**	**nagyon nagy**
nn (nagyon nagy)	kicsi	kicsi	nagy	**nagyon nagy**	**nagyon nagy**	**nagyon nagy**

- Konkrét értékek esetén a kockázat a bekövetkezési valószínûség és a kár egyszerû szorzata. Ez az egyszerû alapgondolat tetszõlegesen finomítható megbízhatósági tényezõkkel vagy statisztikai eljárásokkal.
- A fuzzy logikával támogatott kockázatelemzés segítségével is a kockázatra konkrét értékeket tudunk megadni.

A kockázatokról összegzést készíteni úgy, hogy az összes veszélyforrás kockázatát valamilyen módon összegezzük, nem tûnik jónak. Ez az összesítés eltakarná elõlünk a lényeget; mely veszélyforrások a legkockázatosabbak, és melyek azok, amelyek vállalható veszélyt jelentenek.

A kockázatok meghatározása az elõbbiek alapján a konkrét esetben:

Minden egyes veszélyforrásra megnézve a kockázati mátrixba foglaltakat, a következõk állapíthatók meg:

- A kockázat nagyon nagy a H_1 és K_1 veszélyforrás esetén, mert a kár súlyossága és az elõfordulási valószínûség is nagyon nagy.
- A kockázat nagyon nagy az Ah_1 veszélyforrás esetén is, mert a kár súlyossága nagy és az elõfordulási valószínûség nagyon nagy.

Az intézkedési terv készítésénél figyelembe kell venni a kár súlyosságát és az elõfordulási gyakoriságot is, például a kiemelt eseményeknél célszerûnek tûnik az Ah_1 (külsõ adathordozók kerülhetnek a számítógépbe) veszélyforrás vizsgálatánál az elõfordulási gyakoriság csökkentésére javaslatot tenni, amit a csekély erõforrás igény indokol.

3.3. Összegzés

Az összegzésben a kockázatelemzést néhány gondolattal egészítem ki.
Nagyon bonyolult szervezetek esetén az adatgyûjtéshez, az adatok kiértékeléséhez **szoftverek** is használhatók. Amennyiben a szoftverek megfelelõ tudományos háttérrel bírnak, akkor a kockázatelemzés tárgyilagossága, eredményessége növelhetõ.

A kockázatkezelésnek figyelembe kell vennie a **bizonytalanság**okat. A bizonytalanságok például a következõkbõl adódhatnak;
- hiányzó adatok,
- nem hiteles adatok (az informatikai rendszer gyenge pontjairól kell információt szereznünk esetleg olyan emberektõl is, akiknek nem áll érdekében a hiányosságok feltárása),
- elõre nem jelzett és nem azonosított veszélyforrások,
- olyan események felbukkanása, amelyekkel kapcsolatban nincsenek sem a gyakoriságra sem a valószínûségre használható adatunk,
- veszélyelemzésnél az adott negatív hatásnak túl sok lehetséges oka van, és bármelyik ok esetén túl sok paramétert kell figyelembe venni.

Minden kockázatbecslésben van valamilyen fokú bizonytalanság, a bemenõ adatok bizonytalanságát a hibaterjedés törvényének alkalmazásával kell figyelembe venni.
A számított vagy más módon meghatározott kockázatokat célszerû kiegészíteni az ismerethiányból vagy más okból származó bizonytalanságok bemutatásával.

Ebben a fejezetben, ahol közvetlen **gyakorlati megvalósítás**sal is foglalkoztam, az informatikai rendszer különleges. A vizsgált szervezet használja a Belügyminisztérium, a Fõvárosi Fõpolgármesteri Hivatal, a Katasztrófavédelmi Fõigazgatóság hálózatát is, de a hálózatok biztonságának garantálása nem feladata. Így a fenyegetõ tényezõk, a veszélyforrások feltárása könnyebb, jobban áttekinthetõ. A Fõvárosi Polgári Védelmi Igazgatóság minõsített adatokat is kezel. Az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény 4. §-ának (1) bekezdésében foglaltak alapján a Polgári Védelem szolgálati titokkörét a Polgári Védelem Országos Parancsnoksági közlemény MK. 1997/76. a Polgári Védelem szolgálati titokköri jegyzékében állapította meg. Ezeket az adatokat arra jogosult személyek a TÜK (titkos ügykezelés rendje) szabályai szerint kezelik, külön helyiségben hálózatokról leválasztott gépen. Mindezek figyelembevételével is a teljes körû analízis, amely nem egy disszertáció hivatkozásaként jelenik meg, ennél sokkal bonyolultabb és szerteágazóbb, az itt bemutatott gyakorlati alkalmazással a kockázatelemzés egy-egy lépését kívántam szemléltetni.

4. Az informatikai rendszer egyes részterületeinek kiemelése és biztonságának vizsgálata

Egy informatikai rendszer teljes körû kockázatelemzése nagy feladat, az áttekinthetõség miatt célszerû valamilyen felosztást végezni. Ebben a fejezetben az egyes részterületek közül a környezeti infrastruktúra, az alkalmazások, a rejtjelezés és a hálózatok sajátos kérdéseivel foglalkozom.

4.1. A fizikai környezet, a környezeti infrastruktúra sajátosságai[35]

Az informatikai rendszer fizikai védelme, az illetéktelenek hozzáférésének megakadályozása, az állandó ellenõrzés az informatikai biztonság alapkérdése. Fizikai védelem alatt a mechanikai, az elektronikai és az élõerõvel történõ védelmet értjük.
A környezeti infrastruktúra elemzése magában foglalja a számítóközpont épületének területét, magát az épületet, az épületben lévõ helyiségeket, átviteli vezetékeket, klíma berendezéseket, vízszolgáltatást, világítást, telefonszolgáltatást, áramellátást és egyéb jellegzetességek elemzését. A szervezet a környezeti infrastruktúra egy-egy területét kiemelten fontosnak, külön elemzését is célszerûnek tarthatja.
A vizsgálandó területek általában a következõk;

- az épület biztonsági rendszere,
- az épület mechanikai állapota,
- a szerverszoba,
- a különösen fontos adattárolók, dokumentumok tároló helyiségei,
- titkos ügykezelés helyiségei,
- számítógépes termek,
- adatátviteli eszközök,
- közmûellátás,
- áramellátás,
- villámvédelem, túlfeszültség elleni védelem,
- tûzvédelem, vízvédelem, sugárvédelem.

A felmérésben a következõ kérdésekre keressük a választ:

- A szervezet önálló épülettel rendelkezik? Amennyiben nem, mennyire elkülönült egy adott épületen belül?
- A kerítések, falak, nyílászárók, rácsok, zárak, biztonsági fóliák, trezorok, biztonsági táskák állapota.

[35] Az MSZ ISO/IEC 17799:2002 Informatika. Az informatikai biztonság menedzselésének eljárásrendje szabvány 7. szakasza A fizikai és környezeti biztonság.

- Hány bejárat van? A kapuk, ajtók nyitását ki mûködteti? Van-e beléptetõ rendszer? A beléptetõ rendszer különbözõ jogosultságokat ad-e? A dolgozók olyan kóddal ellátott kártyával rendelkeznek-e, amelynek segítségével a ki és belépés regisztrálható és követhetõ-e az épületben való mozgás?
- A beléptetõ rendszert milyen szoftver mûködteti? Ki tartja karban a rendszert? Hol van a mûködtetõ szerver? Elkülönített-e a szervezet számítógépes rendszerétõl, kapcsolódik-e valamilyen hálózathoz?
- Rendelkezik a szervezet parkolóval? Kik használhatják, és hogyan lehet a parkolóba bejutni?
- Az épületben mûködik-e állandó biztonsági szolgálat?
- A szervezethez nem tartozók beléphetnek-e az épületbe? Ha igen, milyen feltételekkel?
- Kamerák, mozgásérzékelõk, vagy más figyelõ eszközök vannak-e az épületben? A kamerák által használt videó szalagokat újra hasznosítják, meddig õrzik? A biztonsági õrök a saját monitorjukon látják-e a felvett anyagot?
- A dolgozók rendelkeznek-e saját fényképpel, névvel, sorszámmal ellátott kitûzõvel? Az épületben jól látható helyen viselik-e ezt a kitûzõt?
- A szerverszoba az épületen belül hol helyezkedik el? Ki léphet be? Elektromágneses kisugárzástól, zavarkeltéstõl védett-e?
- A szerverszoba megfelelõ hõmérséklete biztosított-e, megfelel-e a tûzvédelmi elõírásoknak? Kamerával, mozgásérzékelõvel egyéb figyelõ eszközökkel felszerelt-e?
- Hol tárolják a kötelezõ mentések adathordozóit, egyéb dokumentumokat? Milyen a tároló szekrény megfelelõsége?
- Az adathordozók, dokumentumok szállításánál, tárolásánál történik-e az idõpontokra vonatkozó rögzítés? A szállításnál megoldott-e a mechanikai és a sértetlenségre vonatkozó védelem? Ki szállítja ezeket az adathordozókat?
- Az adatátviteli eszközök védelme megoldott-e?
- A közmûellátás zavarának kiküszöbölésére tett intézkedések megfelelõk-e?
- Az energiaellátásra redundáns rendszereket hoztak-e létre? Egy ilyen rendszer a következõ fõ modulokból áll; többszörös, független táplálási útvonal, a betáplálások különbözõ földrajzi vonala, alternatív üzemanyagok használata, tartalék generátorok, szünetmentes áramellátó berendezések. [16]
- Megfelelõ szünetmentes áramellátót alkalmaznak-e? A *line-interaktív*[36] és *delta-konverziójú*[37] berendezések a hálózati tápenergia hiányosságait a feszültségeltérést, a

[36] Egyike a legegyszerûbbeknek a line-interaktív felépítés. Itt az UPS nem végez energiaátalakítást, a bemenet (a táphálózat) mûködés közben általában összeköttetésben van a kimenettel, jelen esetben a számítógéppel. Alapállapotban az UPS kimenetéhez kapcsolt fogyasztó közvetlenül a hálózati tápenergiát kapja, amelynek minõségét képes az UPS kis mértékben korrigálni. Inverteres, azaz akkumulátoros üzemmódba csak áramkimaradás esetén kapcsol át. A kimeneti frekvencia a hálózati frekvenciától függ.

torzítást és a fogyasztó által keltett torzításokat kompenzálja. A *kétszeres konverziójú, online*[38] szünetmentes áramforrásokon ezeken kívül a frekvencia-eltérés sem juthat át.
- Tûzvédelem, vízvédelem, sugárvédelem megvalósulása.
- Az objektum megfelel-e az idevonatkozó szabványok elõírásainak a külsõ villámvédelem kiépítettségében és az elektromágneses villámimpulzus elleni védelem kialakításában?

Az elvárások megismerésénél meg kell tudnunk, hogy az adott rendszer milyen adatokat kezel és ezek az adatok milyen biztonsági osztályba tartoznak. Az alap, fokozott és kiemelt osztályok infrastruktúrájára megadott elvárások vannak, a falak vastagságára, szilárdságára, a nyílászárókra, az elektronikus jelzõrendszerre, a személyi felügyeletre, a kisugárzás elleni védelmi intézkedésekre vonatkozóan. Továbbá a rendszer üzemeltetõjének az idevonatkozó belsõ szabályzatát is figyelembe kell venni.

4.2. Az informatikai alkalmazások kockázatelemzése[39]

Az informatikai alkalmazások megfelelõ szintû mûködése kiemelten fontos területe az informatikai biztonságnak, ezért nagyobb részletességgel foglalkozom az igényelt rendelkezésre állással, a becsült anyagi kárral, a meghibásodási valószínûségekkel. A megfelelõ pontértékekbõl egy kockázati mátrix segítségével a kockázat megadható.
Informatikai alkalmazás valamely informatikai rendszer olyan feladatok teljesítésére történõ bevezetése, amelyek egy meghatározott, behatárolt szakmai és szervezeti területre esnek és közös jegyeik révén tûnnek ki.
Az informatikai kockázatelemzéshez meg kell határozni a felhasználói igényeket, a jelenlegi informatikai rendszer által nyújtott szolgáltatásokat, a hibák elõfordulásának gyakoriságát, az okozott kárt, a rendelkezésre állási igényeket.

A vizsgálandó alkalmazások általában a következõk;
- a szervezet mûködéséhez és üzleti folyamatihoz szükséges alkalmazások,
- a szervezet központi rendszereit támogató alkalmazások,
- a szervezeti egységnél használt egyedi fejlesztésû alkalmazások,
- irodai alkalmazások (Word, Excel, Power Point, Access stb.),

---

[37] A *delta-konverziójú* berendezés esetén is közvetlen összeköttetés van az UPS bemenete és a fogyasztó között, így a frekvencia-eltérés átjuthat rajta, az inverterei párhuzamosan vannak kapcsolva a hálózattal.

[38] A *kétszeres konverziójú, online* szünetmentes áramforrás folyamatosan átalakítja az energiát. Az egyenirányító és az inverter folyamatosan üzemel. A kétszeres átalakítás (AC-DC, DC-AC) miatt a hálózati zavarok nem jutnak a fogyasztóra, így a fogyasztó stabil, szünetmentes tápenergiát kap.
DC-AC: egyen-váltó átalakító.

[39] Az informatikai alkalmazások kockázatelemzésének eljárását a KÜRT COMPUTER RENDSZERHÁZ RT biztonsági szakemberivel (Papp Attila, dr. Remzsõ Tibor) való konzultáció alapján alakítottam ki.

- fájlszerverek, hálózati könyvtárak,
- elektronikus levelezés,
- internet elérés,
- intranet elérés.

Az egyes szervezeti egységeknél használt alkalmazások feltérképezéséhez ismertetni kell a felmérés témaköreit, majd ezután nyomtatványok (7. számú melléklet) kitöltetése tûnik a legcélravezetõbb megoldásnak, de a táblázat mezõinek értelmezését mindenképpen mellékelni kell a nyomtatványhoz.

A felmérésben a következõ kérdésekre keressük a választ:

- Milyen folyamatokhoz kapcsolódik a szervezeti egység feladata? Ezek a folyamatok mennyire fontosak, mekkora fontosságúak a szervezet életében?
- Milyen informatikai alkalmazásokat használnak, ezekhez milyen informatikai rendszerelemek kapcsolódnak (munkaállomások száma, típusa, LAN/WAN/Internet/egyéb külsõ kapcsolatok, tárolóegységek, mentõegységek, hálózati aktív és passzív elemek, kiszolgálók)?
- Az egyes alkalmazásokat mennyien és mennyi ideig használják egy átlagos munkanap során?
- A napi munkavégzéshez mennyire szükséges az informatikai rendszerek rendelkezésre állása? Az adott folyamatot milyen mértékben és mennyi ideig lehetne kiváltani helyettesítõ eszközökkel, kézi feldolgozással, külsõ segítség igénybevételével stb.?
- Milyen anyagi, jogi, erkölcsi jellegû veszteséggel járhat az egyes alkalmazásokhoz kapcsolódó különbözõ folyamatok kiesése.
- Megoldható-e a különbözõ kiesõ rendszerek helyettesítése?
- Mennyi ideig tudják nélkülözni a különbözõ alkalmazásokat, ha nincs lehetõség helyettesítésre? Mennyi ideig tudják nélkülözni az adott alkalmazást, helyettesítõ eszközök igénybevételével?
- Milyen tapasztalatokkal, észrevételekkel rendelkeznek a különbözõ informatikai rendszerekkel kapcsolatban?
- Milyen gyakran következnek be fennakadások, problémák az informatikai rendszerben, és ezek mennyi ideig tartanak?
- Elõfordult-e már jelentõs rendszerleállás? Ha igen, mikor, milyen idõtartamra, és mely alkalmazásokat, folyamatokat és területeket érintett? A kiesés milyen anyagi és egyéb jellegû veszteséget okozott? Felmérték-e a veszteségeket?
- Használnak-e egyedi fejlesztésû, speciális alkalmazásokat? Ha igen, akkor ki fejlesztette, milyen programnyelven írták, milyen környezetben futnak, milyen célra használják és ki felügyeli ezeket?
- Hol tárolják az adataikat? Az adatokat jellemzõen a helyi gép merevlemezére, vagy hálózati meghajtóra mentik? Amennyiben bizalmas jellegûek az adatok, ki és

hogyan férhet hozzá? Hogyan történik a jogosultságok beállítása, meghatározása, ki kérheti és ki végzi ezeket a mûveleteket?

- Készítenek-e biztonsági mentést az adataikról? Milyen gyakorisággal és milyen módszerrel? Alapvetõen két mentési eljárás közül választhatunk: a teljes mentés a szerver minden adatára vonatkozik, míg a *növekményes (inkrementális vagy különbségi)* mentés csak a legutolsó mentés óta változott adatokra. A teljes mentés jelentõs elõnnyel jár, a korábbi állapot igen gyorsan helyreállítható. A növekményes mentést is rendszeresen végzik, de a megváltozott adatok nem írják felül az elõzõ mentés adatait. A háttértárolón így egymás után több mentés adatai megtalálhatók, ami a helyreállításnál több részmentés visszaállítását követeli meg.
- Elõfordult-e már adatvesztés?
- Tárolnak-e bizalmas adatokat a különbözõ rendszerekben? Ha igen, milyen jellegûeket?
- Hogyan valósul meg az informatikai tevékenység szabályozása és dokumentálása?
- Hogyan rangsorolják fontosság alapján az általuk használt informatikai alkalmazásokat a munkavégzésükhöz kapcsolódó nélkülözhetetlenségük szempontjából?
- Mely alkalmazásokat/ rendszereket tekintenek kritikus fontosságúnak?

A kérdésekkel kapcsolatos táblázat mezõinek értelmezése: (a teljes táblázat 7. számú melléklet)

Alkalmazás megnevezése: Az adott táblázat melyik alkalmazásra vonatkozik? A táblázatot minden rendszeresen használt alkalmazásra ki kell tölteni.

Fejlesztõ megnevezése: az adott alkalmazást fejlesztõ vagy készítõ cég vagy belsõ szervezeti egység megnevezése.

Az alkalmazás hatása a szervezet munkájára:

Annak a meghatározása, hogy az alkalmazás kiesése milyen közvetlen vagy közvetett hatással van a szervezet mûködési rendjére:

- Alacsony, közepes, magas lehet a kiváltott hatás mértéke.
- Közvetlenül vagy más folyamatokon keresztül van hatással az adott alkalmazás a szervezetre.

Kritikus idõszakok: annak a meghatározása, hogy az adott alkalmazásra vonatkozóan a szervezeti egységnél létezik-e olyan idõszak, amely során nem pótolható a rendszer kiesése.

Becsült kárérték a kiesés miatt: annak a meghatározása, hogy a szervezeti egységnél mekkora értékû és milyen jellegû közvetlen és közvetett anyagi kár keletkezhet az adott alkalmazás 1 munkanapi (8 óra) kieséséhez kapcsolódóan.

Szervezeti egység megnevezése:

Az adott táblázatot kitöltõ válaszadó szervezeti egység szerinti besorolása.

Felelõs megnevezése:
Az adott alkalmazás üzemeltetéséért, karbantartásáért, a fejlesztõkkel való kapcsolattartásért felelõs személy, szervezeti egység megnevezése.
Hatás a szervezeti egység mûködésére:
Annak a meghatározása, hogy az alkalmazás kiesése milyen közvetlen vagy közvetett hatással van a szervezeti egység mûködési rendjére.
Megengedett maximális kiesési idõ:
Az adott alkalmazással szemben a szervezeti egységnél megengedhetõ maximális kiesési idõ.
Fontossági sorrend: Az adott alkalmazás fontossági besorolása a szervezeti egységnél. A fontosság meghatározásánál szükség van a napi munkavégzés idejére és az alkalmazás kiesése miatt bekövetkezõ anyagi és nem anyagi jellegû veszteségek mértékére.
Kritikus alkalmazás: Az adott alkalmazás a szervezeti egység normális mûködési rendjének fenn-tarthatósága szempontjából kritikus-e?
Központi alkalmazás / Egyedi fejlesztés:
Annak meghatározása, hogy az adott alkalmazás egy vagy több szervezeti egységnél használatos-e.
Felhasználók száma:
Az adott alkalmazás felhasználóinak száma a válaszadó szervezeti egységnél.
Helyettesíthetõ:
Az alkalmazás a szervezeti egységnél helyettesíthetõ-e? Ha igen, akkor milyen mértékben; részben vagy teljesen (a megengedett maximális kiesési idõre vonatkozóan).
Hibák elõfordulási gyakorisága:
Az adott alkalmazásnál szervezeti szinten milyen gyakran tapasztaltak hibákat, rendellenes mûködést.
Felsõbb szinten megengedett maximális kiesési idõ:
Az adott alkalmazással szemben a szervezetnél megengedhetõ maximális kiesési idõ.
Rendelkezésre állási kategória:
Az adott alkalmazásra vonatkozó rendelkezésre állási kategória, amelyek a különbözõ rendszerekkel szemben a szervezeti szinten megengedhetõ maximális kiesési idõk kategóriákba sorolásával képezhetõk.

A válaszadáshoz felhasználható skálák:

Az igényelt rendelkezésre állás, éves szinten		
Megengedett kiesési idõ	**Rendelkezésre állás %-a**	**Skálaérték**
Évi 5 percnél kevesebb	99,999 %	1
Évi 30 percnél kevesebb	99,995 %	2
Évi 1 óránál kevesebb	99,99 %	3
Évi 4 óránál kevesebb	99,95 %	4
Évi 1napnál kevesebb	99,9 %	5
Évi 3 napnál kevesebb	99 %	6
Évi 1 hétnél kevesebb	97,5 %	7
Évi 2 hétnél kevesebb	95 %	8
Évi 4 hétnél kevesebb	92,5 %	9
Évi 1 hónapnál több	90 %	10

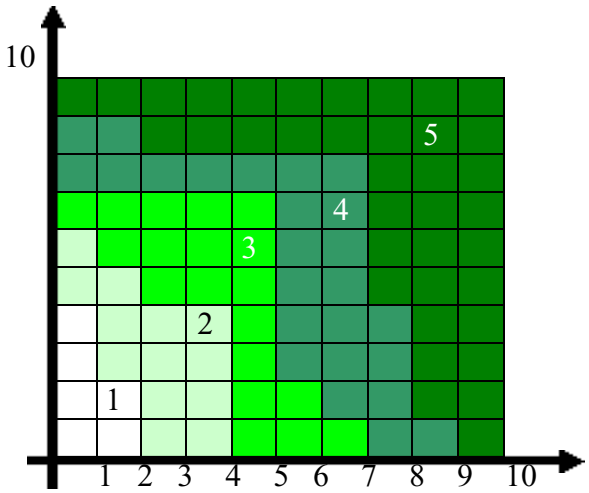
Éves szinten bekövetkezõ becsült anyagi kár	
Becsült kárérték (Ft)	**Skálaérték**
1-1 000	1
1 001-1 0000	2
10 001-30 000	3
30 001-100 000	4
100 001-300 000	5
300 001-1 000 000	6
1 000 001-3 000 000	7
3 000 001- 10 000 000	8
10 000 001-30 000 000	9
30 000 001-	10

Meghibásodások elõfordulási gyakorisága	
Gyakoriságok	**Skálaérték**
Óránként	10
Naponta többször	9
Naponta	8
Hetente többször	7
Hetente	6
Havonta többször	5
Havonta	4
Évente többször	3
Évente	2
Két vagy több évente	1

A kockázat meghatározása:

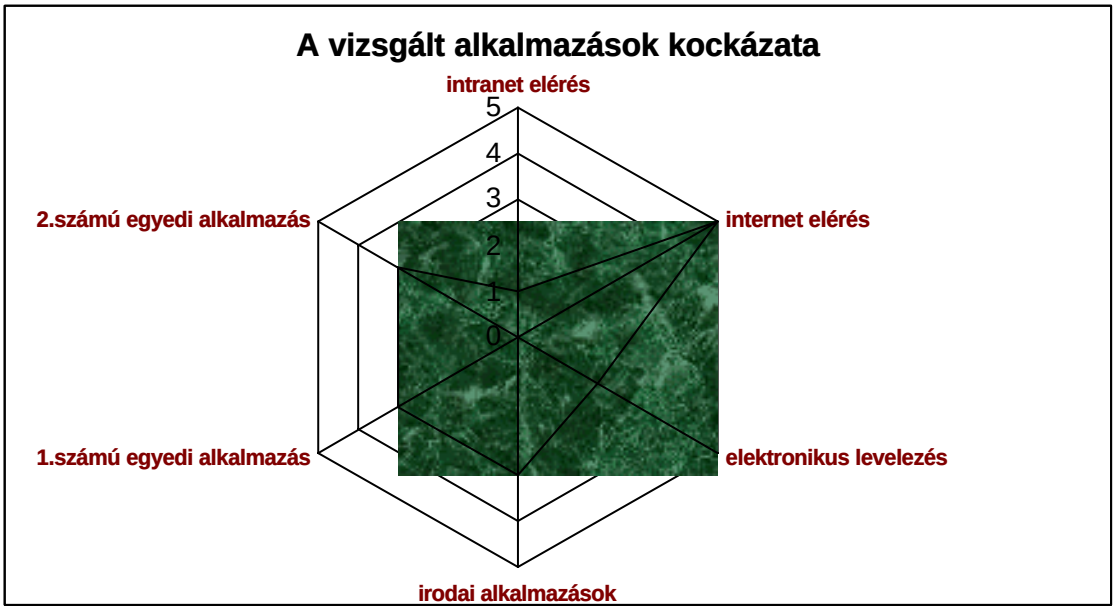
A kockázat kiértékelésénél az elviselhetõség meghatározásánál átgondolt döntés szükséges, ami figyelembe veszi az igényelt rendelkezésre állást, ennek több lehetséges módja van. A kockázati mátrix megszerkesztése után a kockázatot kvalitatív módon is értékelhetjük, de a konkrét helyzet figyelembevételével számokat is rendelhetünk a kockázathoz, például az alábbi táblázat alapján. Ennek az elõnye, hogy az

elviselhetetlen, tehát az intézkedéseket kívánó kockázatok között is látványosabb különbség tehetõ.



Az alkalmazások kockázatának megjelenítése:

A kockázatok kvantitatív értékelése esetén, az egyes alkalmazások kockázatát a szemléletesség érdekében ábrázolhatjuk, így kitûnik például az alábbi példában, hogy az internet elérés biztonságának növeléséhez feltétlen döntéshozás szükséges.



Ahol a kockázat elviselhetetlen, fel kell tárni a hiba okát és a kockázatszabályozás folyamatában az elvárt rendelkezésre állásnak megfelelõen intézkedések meghozatala szükséges, és javasolni kell az egyes intézkedések erõforrás igényét is.

Az intézkedések fontosságára különbözõ szinteket adhatunk meg:

- *Alapfontosságú* azoknak a kockázati tényezõknek a kiküszöbölése, amelyek a rendszer elvárt rendelkezésre állását nem veszélyeztetik, de hatásuk olyan nem

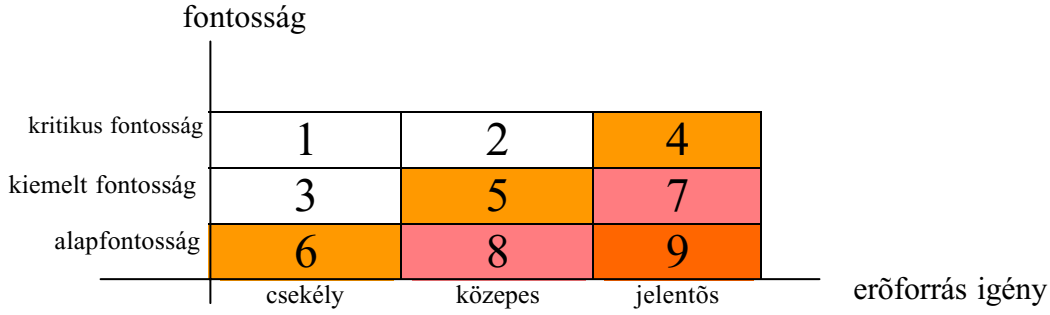
kívánt eseményekhez vezethet, amelyek elhárítása elõre nem tervezett többlet ráfordítást igényel az adott szervezet részérõl.

- *Kiemelt fontosságú* azoknak a kockázati tényezõknek a kiküszöbölése, amelyek közvetve veszélyeztetik a rendszer elvárt rendelkezésre állását, és olyan hatásuk lehet, amelyek hosszú távon veszélyeztetik a rendszert, és káresemények bekövetkezéséhez vezethetnek.
- *Kritikus fontosságú* azoknak a kockázati tényezõknek a kiküszöbölése, amelyek azonnal és közvetlenül veszélyeztetik a rendszer elvárt rendelkezésre állását, a tevékenységének folyamatosságát és fenntarthatóságát.

Az erõforrás-igény jelenti azoknak a személyi és tárgyi erõforrásoknak az összességét, amely egy adott kockázati tényezõ kiküszöböléséhez szükséges. Eszerint:

- *Csekély erõforrás igényt* jelent, ha a kockázati tényezõ kiküszöbölése egy adott szervezeti egység saját hatáskörén belül megoldható, ez humán erõforrás igénybevételét, az erõforrások esetleges átcsoportosítást, hatékonyabb felhasználást foglalja magába.
- *Közepes erõforrás igényt* jelent, ha a kockázati tényezõ kiküszöbölése egy adott szervezeti egység szintjén már nem, csak szervezeti szinten oldható meg.
- *Jelentõs erõforrás igényt* jelent, ha a kockázati tényezõ kiküszöbölése egy adott szervezeti szinten is csak elõre tervezett módon oldható meg, mert megfelelõ pénzügyi forrásokat kell rá elkülöníteni.

Az intézkedések végrehajtási sorrendje a fontosság és az erõforrás függvényében adható meg. A fontosságot és az erõforrás igényt egy 3x3 (mivel a fontosságot is és az erõforrás igényt is három szakaszra osztottuk) mátrixban adjuk meg.



1-2-3 operatív jellegû megvalósítás:

Ebbe a csoportba azok az intézkedések tartoznak, amelyek kritikus fontosságuk és csekély vagy közepes erõforrás igényük miatt rövid idõn belül megvalósíthatók.

4-5-6 taktikai jellegû megvalósítás:

Ebbe a csoportba azok az intézkedések tartoznak, amelyek kiemelt fontosságuk és csekély vagy közepes erõforrás igényûk miatt nem valósíthatók meg azonnal.

7-8-9 stratégiai jellegû megvalósítás:

Ebbe a csoportba azok az intézkedések tartoznak, amelyek alapfontosságúak és erõforrás igényük közepes vagy jelentõs. A feladatot tervezni kell, a megvalósításhoz külön pénzösszegek elkülönítése szükséges.

Összességében hangsúlyozni kell, hogy az informatikai alkalmazások biztonságának ilyen részletességgel történõ vizsgálata szükséges, a fontosságuk, a nagyságrendjük, a szervezeti jelentõségük miatt. Ezen kívül az alkalmazásoknál leírt tényezõket más részterületen is lehet használni, gondolok itt a rendelkezésre állás felmérésére, az elõfordulási gyakoriság, a becsült anyagi kár táblázataira, a bevezetendõ intézkedések vizsgálatára.

4.3. A rejtjelezés kockázatelemzése[40]

A rejtjelezés alapvetõ feladata algoritmikus eszközökkel biztosítani azt, hogy védett adatok csak az azok felhasználására kijelölt körben legyenek érthetõk. A kriptográfiának nem az egyetlen célja, hogy egy adott rejtjelezett szöveg elméletileg feltörhetetlen legyen, a hangsúly a gyakorlati feltörhetetlenségen van. Olyan nehézségû rejtjelezést kell választani, hogy egy esetleges feltörési kísérlet erõforrás igénye (pénz, idõ, emberi erõforrás) nagyobb legyen, mint a feltört információból elérhetõ haszon. Minél hosszabb a rejtjelezéshez használt kulcs, megfelelõen választott rejtjelezõ algoritmus esetén a feltörés, annál több erõforrást vehet igénybe. Az információk értékessége, különbözõsége miatt nincs egyetlen, minden helyzetben használható, szabványosított rejtjelezõ algoritmus. A különbözõ típusú eljárások különbözõ területekre alkalmasak, vannak olyan rejtjelezõ módszerek, amelyek egy erõsebb géppel (rövid kulcs esetén) akár pár nap alatt feltörhetõk, de kis erõforrás igényûek, és nem igényelnek nagy infrastruktúrát, így jól használhatóak egy olyan kommunikáció esetén, melynél a küldött információ ennél kevesebb idõ alatt elévül. A biztonsági kérdések esetén különösen fontos, hogy tudomást szerezzünk arról, ha az alkalmazni kívánt eljárást feltörték.

Alapvetõen kétféle rejtjelezési módszer használatos, a szimmetrikus kulcsú és az aszimmetrikus kulcsú.

A *szimmetrikus kulcsú algoritmusok* közös jellemzõje, hogy a kódolásra és a dekódolásra ugyanazt a kulcsot használják. Ennek a módszernek az alkalmazásánál mind a küldõ félnek, mind a fogadó félnek ismernie kell a kulcsot. Az alkalmazáshoz a használat megkezdése elõtt meg kell állapodni egy közös kulcsban, és azt titokban kell tartani, az üzeneteket csak a titkos kulcs segítségével lehet dekódolni. A szimmetrikus

[40] A rejtjelezés és a titkosítás fogalmát a polgári életben gyakran azonosnak tekintik. A titkosítás az információ-visszatartását jelenti, pl. titkosítani; iratokat a nyilvánosság számára hozzáférhetetlenné tenni. A rejtjelezés az ITB 8. számú ajánlása szerint az adat titkosírással történõ átalakítása.

kulcsú rejtjelezési módszerek hátránya pontosan a titkosan kezelendõ kulcsban van, amelyet egy biztonságos csatornán kellene elküldeni. A titkos kulcs cseréje a szimmetrikus algoritmusok esetében megoldható, de az elõbbi problémák miatt elterjedtebb megoldás a nyilvános kulcsú, aszimmetrikus rejtjelezés használata. A biztonság követelményeinek a szimmetrikus eljárással rejtjelezett dokumentumok csak bizonyos megszorításokkal felelnek meg.

A szimmetrikus rejtjelezési eljárások elõnyei:

- A szimmetrikus eljárásoknak nagy szakirodalma, történelmi elõzménye van. A gyakorlati és elméleti ismeretek bõvülése vezetett el az 1970-es évek DES algoritmusáig is.
- Az alkalmazott kulcsok viszonylag rövidek.
- A szimmetrikus algoritmusok gyorsak, így jól használhatók olyan alkalmazásokban, melyek nagy adatátviteli sebességet igényelnek. A mai technikai viszonyok között nem megfejthetetlenek, de megfelelõ hosszúságú kulcs esetén a feltörésnek nagy az idõigénye.

A szimmetrikus rejtjelezési eljárások hátrányai:

- A megfejtési kulcsoknak mind a feladó, mint a címzett oldalon titokban kell maradniuk, egészen a kommunikáció végéig.
- Az olyan szervezetekben, ahol sokan kívánnak egymással érintkezésbe lépni, a kulcsok száma a résztvevõk számával négyzetesen arányos.
- A feleknek a kommunikációs folyamatok megkezdése elõtt kulcsot kell cserélniük egy biztonságos csatorna használatával és minden kulcs-cserénél fennáll a lehallgatás veszélye.
- Az alkalmazott kulcsok viszonylag rövidek, ez nemcsak elõnyt hanem egy bizonyos szempontból hátrányt is jelent, a brute force[41] támadások a rövid kulcsoknál a legveszélyesebbek, így a kulcsokat sûrûn kell cserélni, a feltételezett feltörési idõ figyelembevételével.
- A sok partner esetén megvalósított gyakori kulcs-csere azonban nagy hálózati forgalmat von maga után.

Aszimmetrikus (nyilvános) kulcsú rejtjelezés elve:

Az adatrejtjelezést le tudjuk írni *matematikai függvénnyel*, amely az eredeti szöveghez (E) a kódolt szöveget (K) rendeli.

f: $E \rightarrow K$

f^{-1}: $K \rightarrow E$ f^{-1} egy dekódoló függvény, f^{-1} az f-nek inverze

A nyilvános kulcsú rejtjelezésnél olyan f kódoló függvényeket keresünk, amelyek számítógépek segítségével belátható idõn belül kiszámíthatók, de az inverz függvényük

[41] brute force, nyers erõ. Ez a feltörési módszer a lehetséges kulcsok végigpróbálgatásán alapul

(f^{-1}) f-bõl belátható idõn belül, adott informatikai eszközökkel nem számolható. Az ilyen függvényeket a szakirodalom egyirányú függvényeknek nevezi.

RSA:

Egy ilyen egyirányú függvényt adott meg Rivest, Shamir és Adleman[42] 1978-ban. A nevük kezdõbetûje alapján beszélünk RSA nyilvános kulcsú rejtjelezési módszerrõl, ez a legismertebb megvalósítása az aszimmetrikus kulcsú eljárásoknak.

Minden X_i személy, aki részt akar venni a titkos információcserében nyilvánosságra hoz egy f_i kódoló függvényt és titokban tart egy f_i^{-1} dekódoló függvényt.

f_i és f_i^{-1}-nek a következõ tulajdonságai vannak:

- Ha H egy hír, akkor $f_i(f_i^{-1}(H))=f_i^{-1}(f_i(H))=H$
- f_i és f_i^{-1} számítógépen könnyen, belátható idõn belül végrehajtható
- belátható idõn belül, gyakorlatilag lehetetlen f_i^{-1} –t az f_i –bõl meghatározni

Hogyan lehet ezzel a módszerrel az *üzenet küldõjét azonosítani*?

> X_i küld X_j- nek egy aláírás szöveget, amit elõször saját f_i^{-1} dekódoló függvényével, utána f_j kódoló függvényével titkosít $f_j(f_i^{-1}(x))$
>
> X_j a kapott üzenetet a saját dekódoló függvényével, majd X_i nyilvános kódoló kulcsával megfejti.

Az RSA nyilvános kulcsú rejtjelezési módszer publikus, bárki számára elérhetõ, a ma ismert egyik legerõsebb módszer.

Az RSA módszer használata:

- Az alkalmazónak két prímszámot (p és q) kell választani.

A módszer annál biztonságosabb, minél nagyobbak a prímszámok. Ki kell választani véletlenszerûen egy több, mint 100 jegyû számot, ezen szám környezetében alkalmazni az Eratoszteneszi szita[43] módszert, az álprímek kiszûrésére különbözõ prímszám tesztek végezhetõk. A valószínûségi tesztek (pl. Miller-Rabin teszt[44]) gyorsak, eredményeik kriptográfiai szempontból megfelelõek, de nem döntik el teljes biztonsággal egy

---

[42] Maga az elképzelés Hellmantól származik, de Rivest, Shamir, Adleman (1978) adta meg a megbízhatónak látszó, technikailag kivitelezhetõ nyilvános kulcsú algoritmust.

[43] Eratoszteneszi szita: A prímszámok megkeresésének egyik módszere. Felírjuk egy tetszõlegesen nagy k korlátig az 1-nél nagyobb természetes számokat és töröljük közülük a 2-vel oszthatókat, a 2-es szám kivételével. Ezután a megmaradó számok közül a legkisebbel (3) megismételjük az eljárást és így tovább mindaddig, amíg csak marad ilyen legkisebb figyelembe nem vett szám. A visszamaradó számok a k-nál nem nagyobb prímszámok. (Matematikai kislexikon)

[44] Miller-Rabin teszt:

1. Legyen $m-1=2^k n$, ahol n páratlan.
2. Válasszunk egy véletlen a –t, ahol $a \in Z$ és $a \in [1,m)$
3. Ha az a^n-1, a^n+1, a^{2n}+1,…, $a^{2^{k-1}n}+1$ számok egyike sem osztható m-mel, akkor megállunk azzal a válasszal, hogy m összetett, különben megállunk azzal a válasszal, hogy m valószínûleg prím.

(Budapesti Mûszaki és Gazdaságtudományi Egyetem, Számítástudományi Tanszék, Katona Gyula Algoritmuselmélet 18. elõadás, 2002)

számról, hogy prím-e. A determinisztikus tesztekkel (pl. Atkin- Morain teszt[45]) eldönthetõ egy szám prím volta.

- Az $n=pq$ és $\varphi(n)=(p-1)(q-1)$ kiszámítása
- Egy olyan e véletlen szám keresése, amely relatív prím $(p-1)$-hez és $(g-1)$-hez is.
- Meg kell határozni az e szám inverzét (d) modulo $\varphi(n)$.

Ekkor teljesül a következõ: $ed \equiv 1$ modulo $\varphi(n)$

Az inverz megtalálása euklideszi algoritmus segítségével történik.

- d a titkos kulcs, n és e közzétehetõ, az a nyilvános kulcs.

Felvetõdik a kérdés, hogy *biztonságosan lehet-e kódolni az RSA módszerrel.*

A feltörések ellen a paraméterek jó kiválasztásával is védekezni lehet:

- A p és q számok nagyságrendje kövesse az informatikai eszközök és a felbontási algoritmusok fejlõdését.
- A p és q számok közötti különbség nagy legyen.
- A $p-1, p+1, q-1, q+1$ számoknak csak nagy prímosztói legyenek.
- A p és q-t a jelenlegi ismereteink szerint a következõképpen célszerû megválasztani: p és q véletlen szám legyen, de emellett még legalább 512 bináris jegyûek legyenek, így n 1024 bites és $p-q$ legalább 511 bináris jegyû legyen.

Eddig még nem bizonyított az RSA biztonsága vagy feltörhetõsége, ez az algoritmuselmélet nagy kihívása. A polgári célú adatvédelem (pl. bankrendszer) nagy része összedõlne, ha olyan algoritmust írnának, amellyel számítógép segítségével egy 300-400-500 jegyû számot *reális idõ* alatt prímtényezõk szorzatára bonthatnánk. Ha azt sikerülne bebizonyítani, hogy nincs ilyen algoritmus, akkor az ezen az elven mûködõ rejtjelezõ módszert nyugodtan lehetne bárhol alkalmazni.

Összetett számok prímtényezõkre bontására számtalan algoritmus létezik. Az algoritmus az n hosszában exponenciális futásidejû (általában). Ha n prímszám, akkor $[\sqrt{n}]$ számot kell ellenõriznie a gépnek, a bemenet mérete n logaritmusával arányos, mivel a méret a jegyek száma.

Futási idõ nagyságrendje: $10^{\text{méret}/2}$ db. elemi mûvelet (összeadás, osztás). Ez egy normálisnak mondható 512 bites kulcs kb. 155 jegyû számra 10^{78}, ami egy Intel Pentium IV processzorral rendelkezõ gépnek $(1{,}2 * 10^9 \frac{\text{mûvelet}}{\text{s}})$ $8{,}3 * 10^{68}$ másodpercet ad, ami $2{,}7 * 10^{61}$ év.

Ha növeljük az RSA rejtjelezésben használt n értékét, olyan értékekhez jutunk, ahol a rejtjelezés folyamata pár másodperc alatt, míg a kulcs ismerete nélküli a feltörés évezredekig, vagy évmilliókig tart a mai számítási kapacitások mellett.

[45] Atkin- Morain teszt: A teszttel 1998 körül egy 500 megahertzes processzorral körülbelül 512 bites számokról tudták eldönteni, hogy prímszámok-e. A mai átlagos processzorok viszont ennél négyszer gyorsabbak, úgyhogy figyelembe véve a 128, 256, 512 bites számok prímellenõrzésének idõadatai által mutatott trendet, ma már vélhetõen az 1024 bites eset is kezelhetõ.

A számítógépek mûveleti sebességének növekedésével idõközönként felül kell vizsgálni a használható és ajánlott *n* értéket, és ennek növelésével ismét biztonságos tartományba kerül a rejtjelezés.

Természetesen létezik más nyilvános kulcsú algoritmus is, mint a leggyakrabban használt és negyed évszázada fel nem tört RSA. Minden nyilvános kulcsú kriptográfiai algoritmus alapja egy matematikai nehéz probléma, amely segítségével egyirányú függvény készíthetõ.

A nyilvános kulcsú rejtjelezés algoritmusai alapjául szolgáló matematikai problémák és felhasználásuk:

- az egész számok faktorizációja, (RSA, RW, LUC,…)
- a diszkrét logaritmus probléma, (DH, DH2, DSA, ElGamal, ECC,…)
- utazó ügynök probléma,
- gráfszínezési probléma,
- Hamilton-út probléma,
- hátizsák probléma,
- elliptikus görbéken alapuló diszkrét logaritmus probléma, (ECDH, ECMQV, ECIES, ECDSA, ECNR, MQV,…)
- rács-redukció,
- egyéb (LUCDIF, LUCELG, LUCRSA, Merkle-Hellmann, Chor-Rivest, NTRU, McEliece,…).

NTRU:

Az NTRU algoritmusát az 1990-es évek közepén fejlesztették ki (Jeffrey Hoffstein, Jill Pipher, Joseph Silverman). Az NTRU ismertetésekben az algoritmus elõnyének a gyorsaságát, skálázhatóságát, rugalmasságát, kicsi számításigényét, az egyszerû programkódot, a jó hardveres megvalósíthatóságot említik.

A matematikailag nehéz probléma, amin az NTRU alapszik, a *Legrövidebb Vektor Probléma* illetve a *Legközelebbi Vektor Probléma.*

Legrövidebb Vektor Probléma (SVP):

A Legrövidebb Vektor Probléma az *n* dimenziós rács esetében megtalálni a legkisebb zérustól különbözõ rácsbeli elemet. Egy *n* dimenziós rácsot a $v_1,v_2,\ldots,v_n$ bázisvektorok segítségével adhatunk meg. Ekkor a rács elemei az $a_1 v_1 + a_2 v_2 + \ldots + a_n v_n$ formában elõálló vektorok, ahol $a_1, a_2, .., a_n$ egész számok.

Legközelebbi Vektor Probléma (CVP):

A Legközelebbi Vektor Probléma az *n* dimenziós rács esetében megtalálni az *n* dimenziós térben adott *w* vektorhoz legközelebb esõ rácsbeli elemet.

A két probléma megfeleltethetõ egymásnak, NP-teljes problémák[46]. A legjelentõsebb gyakorlati eredmény a rács redukció módszere (L3 algoritmus), amely nem a legkisebb, hanem egy elegendõen kicsi vektort keres meg a rácsban, a dimenzió függvényében polinom idõben. A legkisebb vektor megkereséséhez exponenciális idõ kell. Az L3 algoritmus ismerete után a gyakorlatban nem voltak elég biztonságosak a korai CVP-alapú kriptográfiai rendszerek, mivel a dimenzió növelésével nagymértékben nõtt a kulcs mérete is, azaz a még használható kulcsméret mellett viszonylag kicsi volt a dimenziószám, ami módot adott a törésre. Az NTRU-nál a kulcsméret nem függ ilyen nagyon a dimenzió méretétõl (n-nel és nem n^2-*tel* arányos), így használható nagyobb, jelenleg 500-1000-es dimenzió.

Az NTRU biztonsága:

- Az NTRU Security Labs 2001-ben, hasonlóan az RSA–hoz, meghirdetett három nehézségi szinten n= 251, n = 347 és n= 503 feladatokat, eddig egyetlen feladatot sem fejtettek meg.
- Az NTRU kriptográfiai rendszer biztonságosságát matematikusok, kriptográfusok tanulmányozzák, több olyan ajánlás született, amelyet a gyártók folyamatosan beépítenek. Például: célszerû n-t prímnek választani.
- A kutatási eredmények alapján a töréshez szükséges becsült idõ n=167 esetén 550 év, n= 503 esetén 5400 év.

Az aszimmetrikus rejtjelezési eljárások elõnyei:

- A résztvevõ feleknek két kulcsuk van, ezek feladata más és más. Az egyiket nyilvánosságra hozzák, ez lesz a kódoláshoz használt kulcs. A másikat titokban kell tartani, ez lesz a dekódoló kulcs. Minden résztvevõnek csak a saját titkos kulcsát kell titokban tartania.
- A nagy létszámú résztvevõ esetén sem jelent problémát a kulcsok megosztása, ha n partner van, akkor n darab nyilvános kulcsot kell kezelni.
- A kulcsokat nem kell gyakran cserélni, mivel az aszimmetrikus algoritmusok nehéz matematikai problémákon alapulnak és kulcsaik jóval hosszabbak, mint a szimmetrikus kulcsok, ezért, egy – egy kulcs évekig használható.
- A nagyon hosszú kulcsok gyakorlatilag lehetetlenné teszik a *brute force* támadást.

[46] A matematikai problémákat különbözõ bonyolultsági osztályokba sorolhatjuk. A P-osztályba tartozó, determinisztikus idõbonyolultságú problémák megoldására létezik polinomiális megoldó algoritmus. Ezek megoldása egy meghatározott számítási módszerrel mindig ugyanannyi idõt igényel.
A nem determinisztikus idõbonyolultságú, azaz non-P problémáknak nincs adott idõn belül biztos megoldása. Ezek egy csoportját NP-nek (non determinisztikus P) nevezzük, polinomidõben tesztelhetõ feladatok tartoznak ide. Ezen belül van még egy kisebb csoport, amelyet **NP-teljes** osztálynak neveznek. Ahhoz, hogy egy probléma NP-teljes, két dolgot kell belátni; egyrészt azt, hogy a probléma NP-beli, másrészt pedig azt, hogy minden NP-beli probléma visszavezethetõ rá.

- Ezek az algoritmusok hatékonyan használhatók digitális aláírásnál (9. számú melléklet), mivel a titkosítás és a visszafejtés folyamata a legtöbb aszimmetrikus rendszerben felcserélhetõ [47].

Az aszimmetrikus rejtjelezési eljárások hátrányai:

- Szükség van egy megbízható harmadik félre (Trusted Third Party = TTP), aki garantálja, hogy a nyilvántartásában szereplõ felhasználónév és a hozzá tartozó nyilvános kulcs valóban összetartozik.
- Az aszimmetrikus rejtjelezõ eljárások általában lassúak, emiatt gyakran a szimmetrikus algoritmusokkal együtt használják õket.
- A kulcsok mérete általában sokkal hosszabb, mint a szimmetrikus algoritmusok 56-128 bites kulcsa (az RSA teljesen biztonságosnak mondott kulcsa 1024 bites), így nagy az erõforrás igénye. Ebbõl következõen a digitális aláírások mérete is hosszabb. A kulcsmenedzsment és egyéb mûveletek nagyobb adatmennyiség mozgatását igénylik, mint a szimmetrikus algoritmusok esetében.
- A legtöbb megoldás valamilyen nehezen megoldható matematikai problémán alapszik, de egyetlen algoritmusnak sem bizonyított a tökéletes biztonsága. Az RSA eljárásban a moduláris hatványozás inverze, a moduláris logaritmus jelentheti a kulcs nélküli dekódolást, azonban ehhez szükség lenne *n* prímtényezõs felbontására, de *n*-t olyan nagyra választják, hogy a tényezõkre bontása elméletileg nem, de gyakorlatilag lehetetlen feladat.

A szimmetrikus és aszimmetrikus kulcsú rejtjelezés elõnyeit és hátrányait végiggondolva, felvetõdik a kérdés, hogy melyiket célszerû alkalmazni, ki lehet-e jelenteni az abszolút jó megoldást. Ahol az adatatok szimmetrikus kulcsú titkosítást követelnek meg, titkos kulcsokat és ahol aszimmetrikus titkosításra van szükség, nyilvános kulcsokat kell alkalmazni, ezenkívül lehetséges a kettõ kombinációja is. A szimmetrikus és aszimmetrikus eljárásokon belül is mérlegelendõ a különbözõ algoritmusok közötti választás. Például az RSA-val szemben az ECC (Elliptic Curve Cryptography) gyorsabb és jóval rövidebb kulcsok kellenek hozzá ugyanazon biztonsági szinthez. A 2048 bites RSA kulcsnak egy kb. 224 bites ECC kulcs, egy 4096 bites RSA kulcsnak pedig egy kb. 256 bites ECC kulcs, így ha az ECC algoritmust használja a rendszer, a rövid kulcsok révén lehetõvé válik 1000 vagy még több független kulcs egy hardverben való tárolása. Ezzel szemben az RSA negyed évszázada

[47] 2001. évi XXXV. törvény az elektronikus aláírásról rendelkezik. A törvény szerint lehetõség van egyszerû elektronikus aláírás, fokozott biztonságú elektronikus aláírás, illetve minõsített elektronikus aláírás használatára. Az egyszerû elektronikus aláírás, amelyet egy elektronikus levél végére bárki, bármilyen módon megtehet. Az utóbbi két esetben viszont az aláírás mögött egy ún. nyilvános kulcsú infrastruktúra áll.

minden feltörési kísérletnek ellenállt, a gyengeségek mindig az implementáció nem körültekintõ, a legújabb eredményeket nem ismerõ alkalmazása miatt léptek fel.

Ha arra gondolunk, hogy a számítógépek és az egész számítástechnikai rendszer fejlõdése negatív módon befolyásolja az aszimmetrikus eljárások biztonságát, akkor meg kell vizsgálni a számítástechnikai eszközök fejlõdésének ütemét.

Moore törvény:

Az Intel egyik alapítója, Gordon Moore hipotéziseit nevezzük Moore törvénynek. Moore a jóslatait nem azonos idõpontban állította (kb.10 éves idõintervallumban).

- Az integrált áramkörre tehetõ tranzisztorok száma évente megkétszerezõdik.
- Az integrált áramkörök kapacitása kétévente megduplázódik. Valójában a mikroprocesszorok hatékonysága minden 18 hónapban kétszerezõdik meg.
- A memóriák vonatkozásában azt állította, hogy a memóriákba integrált alkotóelemek száma két és félévenként duplázódik meg. Ez azt jelenti, hogy a memória áramkörök és a mikroprocesszorok fejlõdése nem azonos ütemû, a processzorok hatékonysága gyorsabban nõ, mint a memóriáké. A gyártók újabb és újabb tároló típusokat dolgoznak ki, hogy a mikroprocesszorok teljesítõképessége kihasználható legyen.
- Moore elképzelései az **exponenciális-növekedésrõl** a mágneses tárolóegységeknél is és az üvegszálas távközlés területén is érvényesülni látszik. Így mondják ki azt az általánosítást, hogy Moore törvénye a számítástechnika növekedésének egészére vonatkozik.

A fejlõdés elõrejelzése:

Az a prognózis, ami folyamatos és ugrásszerû fejlõdés váltakozásának elemzésén alapul, eddig érvényesnek bizonyult. Folyamatos változásnak tekinthetõ az egyes technológiák állandó jellegû fejlesztése, az adott megoldások tökéletesítése. Ugrásszerû emelkedést váltanak ki az olyan nagy sikerû találmányok, mint az 1948-ban feltalált tranzisztor vagy az 1959-ben felfedezett integrált áramkör.

Az, hogy egy konkrét feltételrendszerben a fejlõdésnek határa van, nem csak a kitüntetett mûszaki paraméter korlátozottságából következik, hanem esetleg egyéb körülményekbõl is. Egy határon túl felléphetnek olyan hatások, amelyek a további fejlesztést megkérdõjelezik. A technológiák magasabb szintjei általában egészen új tudományos eredményekre támaszkodnak. Az ilyen áttörések pedig megjósolhatatlanok, vagy csak nagy hibaszázalékkal prognosztizálhatók.

Vannak olyan kijelentések, amelyeket eddig nem cáfolt meg az idõ, pl. hogy a processzorok teljesítménye 18 hónap alatt megduplázódik. Többek, például Stan Williams (a HP vezetõ tervezõje) szerint ez az ütem a közeljövõben lassulni fog, mert az egyre kisebb áramköri lapkákat eredményezõ szilícium alapú MOSFET[48] technológia már nincs messze a kvantum-mechanika által állított határoktól.

[48] MOSFET: Metal-Oxide-Semiconductor Field Effect Transistor, Fém-oxid-félvezetõ térvezérlésû tranzisztor.

Az RSA és más matematikailag nehéz problémán alapuló algoritmusok feltörhetõségével kapcsolatban a következõket kell figyelembe vennünk:

- Az elkövetkezendõ években a számítógépek egyre gyorsabbak lesznek, és egyre könnyebben lehet õket hálózatba kapcsolni. Ezáltal egyszerûbbé válik a rövid kulcsú titkosítások feltörése csupán azzal, hogy végignézik az összes lehetõséget, a brute force technikával.
- Az RSA-nál a 1024 bites vagy annál nagyobb kulcsok belátható idõn belüli feltörhetõségének elvi kérdése a matematikai kutatások napirendjén van, a matematikusok szerint néhány év vagy egy-két évtized múlva várható a megoldás.
- A kvantumszámítógépek (vagy más hasonló gyorsaságú gépek) 2020-ig felváltják a mai tranzisztoros gépeket, egy ilyen gép az RSA 1024 bites kulcsának feltörését néhány perc alatt képes elvégezni.
- A szoftvereket állandóan, folyamatosan fejlesztik.

A gyakorlatban az adatok illetéktelenek kezébe jutásának általában a rejtjelezés feltörhetõségén túl, sokkal inkább a kommunikációs csatorna nem megfelelõ védelme vagy emberi tényezõk, az adatkezelés nem megfelelõen biztonságos szervezése az oka.

A kommunikációs csatorna védelme:

Bármely kommunikáció során információ jut el a küldõ féltõl a címzett félnek egy kommunikációs csatornán keresztül. Az informatikai rendszert alkalmazó kommunikáció során az információ egy része tárolódik a küldõ, illetve a fogadó számítógépes rendszerén is. A védelemnek így ki kell terjednie az információ, a kommunikációs csatorna, illetve a kapcsolattartó felek számítógépeinek biztosítására.
Egy kommunikációs csatorna biztonsága három szinttel jellemezhetõ:

Nem biztonságos csatorna:	**Biztosított csatorna:**	**Fizikailag biztonságos csatorna:**
A támadó csatlakozni tud a csatornához, és rajta áramló információt tetszés szerint megismerheti, törölheti, megváltoztathatja. Ez azt jelenti, hogy az ilyen csatornákon küldött és nem rejtjelezett adatokat bárki elolvashatja,	A támadó fizikailag hozzáférhet a csatornához, így a rajta folyó kommunikációt le tudja hallgatni. Ennek kivédésére rejtjelezõ, illetve az adatintegritást biztosító protokollokat használnak, melyek	Az ilyen kommunikációs csatornákat fizikailag biztosítják oly módon, hogy a támadó fizikailag nem fér a csatornához. A csatornához való kapcsolódáshoz a támadónak a fizikai védelmet meg kell bontania, mely megfelelõ monitorozással figyelhetõ. Egy lehetséges megvalósítás, ha a fizikai védelem feltörése több idõt vesz igénybe, mint ami a támadás érzékelése és az elhárítása között eltelik. A fizikailag biztonságos csatorna elõnye a lehallgathatatlanság magas szintû biztosítása, hátránya hogy kivitelezésének

illetve tartalmukat megváltoztathatja.	megfelelően védik az információt törlés, illetve változtatás ellen.	magas költségei miatt viszonylag csak kis távolságokra telepíthető. Alkalmazása főleg védelmi szervezeteknél, illetve nemzetbiztonsági szolgálatoknál jellemző.

Az elektronikus kommunikációban való részvétel fenyegető tényezői:

Passzív eljárások, amelyek nem változtatják meg az üzenet tartalmát:

- *Forgalomelemzés;* a lehallgató az üzenetváltás tényéből, gyakoriságából, a résztvevő felek ismeretéből jut információhoz.
- *Üzenetfeltörés;* ha egy illetéktelen személy lehallgatja mások üzenetváltását.
- *Üzenettagadás*; ha a kommunikációban résztvevő letagadja a küldés vagy fogadás tényét vagy tartalmát, a kommunikáció időpontját és így tovább.

Aktív eljárások, amelyek megváltoztatják az üzenet tartalmát:

- *Üzenetmódosítás;* ha illetéktelen személy a megszerzett üzenetet megváltoztatva juttatja el a címzetthez.

  A következők nem feltétlenül járnak az üzenet tartalmának megváltoztatásával, de az üzenetküldés menetébe való aktív beavatkozást jelentenek.
- *Színlelés*; ha a küldő vagy a fogadó más személynek adva ki magát, megtéveszti a kommunikációban részt vevő partnerét.
- *Visszajátszás;* ha illetéktelen az eredeti üzenetet megszerzi, és azt megismételve, módosítás nélkül eljuttatja a címzetthez.
- *Üzenetlopás;* ha illetéktelen az eredeti üzenetet megszerzi, és a címzetthez jutását megakadályozza.
- *Üzenetkésleltetés*; ha illetéktelen megszerzi az eredeti üzenetet, és a címzetthez jutását késlelteti.
- *Üzeneteltérítés;* ha illetéktelen megszerez egy üzenetet, és azt nem az eredeti címzetthez juttatja el.

Visszatérve a kommunikációs csatornákról a rejtjelezésre, amelyet akkor tekintünk feltörhetőnek, ha

- a kódolt szövegből meg lehet határozni a kulcsot vagy a kulcs nélkül is a nyílt szöveget,
- a nyílt szöveg és a hozzátartozó rejtett szöveg egyes részleteiből meghatározható a kulcs.

A Denning[49] modell szerint négy alapvetõ támadási módszert különböztethetünk meg:

1. A rejtjelezett szöveg elleni támadás:

A támadó a nyílt szöveget nem, csak a rejtjelezettet ismeri, gyakran van lehetõség a szövegre való következtetésre, például az üzenetnek rögzített formátumú fejlécébõl, szokványos kezdésébõl és befejezésébõl, a gyakori szavakból, szófordulatokból.

2. Ismert nyílt szöveget alkalmazó támadás:

A támadó vagy pontosan ismeri, vagy elég nagy valószínûséggel következtetni tud arra, hogy a titkosított szöveg bizonyos része milyen nyílt szövegbõl állt elõ. Ekkor az a feladata, hogy meg kell fejtenie a rejtjelezett szöveg többi részét az elõbbi információk segítségével. Ezt úgy lehet megtenni, hogy az ismert szövegbõl, vagy az abban elõforduló adatokból vagy rövidítésekbõl és azok rejtjelezett formájából, meghatározzák a rejtjelezõ kulcsot.

3. Választott nyíltszöveget alkalmazó támadás:

- Ha a támadónak módja van arra, hogy tetszõleges, általa választott nyílt szöveget és annak a rejtjelezett alakját is megismerje, akkor meg tudja határozni a rejtjelezés kulcsát. Néhány rejtjelezõ módszer különösen sérülékeny az ilyen jellegû támadásokkal szemben, például a nyilvános kulcsú RSA is. Nagy veszélyforrás, ha a nyílt szöveg és a titkosított változata egy potenciális támadóhoz kerül.
- Ha a támadónak módja van valamilyen adatot elhelyezni, módosítani vagy törölni az adatbázisból, akkor megvizsgálja, hogy ennek a hatására milyen változás történik a rejtjelezett adatbázisban, majd ennek segítségével próbálja a kulcsot megfejteni.

4. Betolakodó támadás:

Amikor két fél kulcsot cserél egymással valamilyen titkos kommunikáció céljára, akkor egy betolakodó támadó beépül a két kommunikáló fél közé és mindkét féllel külön-külön kulcsot cserél. Így mindkét fél más-más kulcsot fog használni és csak a betolakodó ismeri mindkét kulcsot, a támadó bármelyik fél üzenetét megfejti, és újra titkosítja a másik fél kulcsával, majd elküldi az eredeti címzettnek. Azon kívül, hogy ilyen módon a támadó minden információt megszerez, a kommunikáló felek nélküle még kommunikálni sem tudnak.

Van-e az ilyen támadás ellen védelem?

Természetesen vannak módszerek a kivédésre, például a Photuris módszer. Mindkét fél kiszámol egy kriptográfiai hash függvényt[50], amikor kulcsot cserélnek egymással, szignálják azt egy digitális aláírási algoritmussal és megküldik az aláírást a másik félnek. A címzett aztán megvizsgálja az aláírás hitelességét, vagyis azt, hogy azt tényleg az általa ismert partner küldte, vagyis ellenõrzi, hogy az aláírásban lévõ hash függvény azonos-e azzal, amit a saját helyszínén kiszámolt.

---

[49] Dr. Dorothy Denning a Georgetown University számítástechnika professzora.

[50] Hash függvény: Olyan transzformáció, amely egy tetszõleges hosszú szövegbõl fix hosszúságú bitsorozatot készít. Ez a bitsorozat jellemzõ az adott szövegre abban az értelemben, hogy más szöveghez szinte biztosan más hash érték tartozik, illetve az adott bitsorozathoz gyakorlatilag lehetetlen olyan szöveget találni, amelynek ez a képe.

Mikor biztonságos a rejtjelezés?

Egy rejtjeles szöveget feltétel nélkül biztonságosnak nevezünk, ha akármennyi rejtjelezett szöveg áll rendelkezésre, akkor sincs elegendõ információ a kódolt szövegben ahhoz, hogy belõle a nyílt szöveget egyértelmûen meg lehessen határozni.

Ha korlátlanul nagy mennyiségû rejtjelezett szöveg áll a rendelkezésünkre, akkor egy kivétellel (ez az egyszer használatos véletlen kódfüzet) minden kód feltörhetõ. Az egyszer használatos véletlen kódfüzetnél alkalmazott kulcs nem ismétlõdõ, véletlen bitsorozat és a kulcsot csak egyetlen üzenethez használják fel, utána megsemmisítik. Minden üzenethez más kulcsot használnak, mert ha két különbözõ nyílt szöveget kódolnának ugyanazzal a kulccsal, akkor ez már támpontot adhatna a megfejtéshez.

Ezért nagyobb érdeklõdésre tarthatnak számot azok a rejtjelezések, amelyek megfejtéséhez akkora gépkapacitás kell, hogy számítás-, memóriaigényük miatt nem valószínû a feltörhetõségük.

Egy titkosírás *számításigény szempontjából biztonságos* vagy erõs, ha a rendelkezésre álló számítási kapacitás vagy idõ nem elég ahhoz, hogy szisztematikus analízissel feltörjék.

A kriptográfiai rendszer biztonságának vizsgálata:

A kriptográfiai rendszer három jól elkülöníthetõ részbõl tevõdik össze:

- Az *algoritmikus rendszer*, amely a rejtjelezés, hitelesítés, partnerazonosítás és egyéb kriptográfiai eljárások matematikai algoritmusait tartalmazza.
- A *kulcsrendszer*, amelynek lényegesebb elemei; a kulcsmenedzsment, a kulcskialakítás, a kulcsképzés.

  A kulcsmenedzsment a központi kulcsellátás induló kulcsainak képzése, betöltése a rendszer elemeibe, valamint ezek idõszakos cseréje.

  A kulcskialakítás biztosítja, hogy a rejtjelezõ és a megoldó oldalak is ugyanazzal a kulcshalmazzal dolgozzanak (üzeneti kulcs, cserekulcs, hierarchiakulcs, nyilvános kulcs stb.) a számítógépes környezet tulajdonságainak optimális kihasználásával.

  A kulcsképzés a rejtjelezést közvetlenül megelõzõ folyamat, amely a kulcskialakítási rendszernek megfelelõen a rendszertõl pillanatnyi kulcsot kér vagy azzal kulcsot fogadtat el.
- A *védelmi rendszer* a teljes kriptográfiai rendszer önvédelmét, a támadások vagy hibázások elleni felkészítettségét, a kulcselosztás folyamatait stb. jelenti. A védelmi rendszer szoftver és hardver elemeket, üzemeltetési vagy rezsimutasítások sorozatát tartalmazza.

A kriptográfiai rendszerek biztonságát a következõ tényezõk befolyásolják:

- az algoritmus biztonsága,
- programozási hibák (hibás függvények, nem megfelelõen kezelt lehetõségek,…),
- szándékos hibák (trójai programok, …),
- gyenge vagy speciális paraméterek választása,

- rossz konfiguráció (nem megfelelõ hosszúságú kulcsméret, …),
- protokollhibák (közbe ékelõdõ támadó, megszemélyesítés, üzenet visszajátszás),
- a matematikai nehéz probléma megoldása,
- kulcstér csökkentése (információk felhasználása,….).

A kockázatelemzésnél vizsgálandó kérdések:

1. Van-e elõírás az elektronikus lehallgatás kivédésére?
2. Van-e lehetõség az elektronikus lehallgatás kivédésére vagy legalább jelzésére?
3. Szabad-e mesterséges zajt alkalmazni?
4. Lehet-e adattömörítést alkalmazni, ha igen, milyen szabványok alapján?
5. Szimmetrikus, vagy aszimmetrikus rejtjelezõ eljárásokat alkalmaznak?
6. Vannak-e elõírt hashing-típusú algoritmusok?
7. Alkalmaznak-e véletlenszám-generátorokat a nyilvános kulcs elõállításához, ha igen, ezek valódi-, pszeudó- vagy hibrid generátorok?
8. Alapvetõ biztonságtechnikai kérdés a kulcsok elõállítási helye, általánosságban két lehetõség kínálkozik a kulcs-párok generálására és mindkettõ rendelkezik elõnnyel és hátránnyal. A két lehetõséget centralizált és decentralizált kulcsgenerálásnak nevezzük. Elemezni szükséges az elõnyöket és hátrányokat.
9. Megbízható-e a kulcsgenerálás?
10. A kulcsgeneráló eszköz fizikailag is megfelelõen védett?
11. RSA esetén megbízható-e a véletlen prímek generálása?
12. Szabályozott-e a kulcsok érvényességének tartama, a kulcsváltás gyakorlata?
13. Vannak-e elõírt nyilvános kulcsú rejtjelezõ eljárások?
14. Dokumentálható-e ezek megbízhatósága, milyen idõtartamra dokumentálható?
15. Milyen irányelvek szabályozzák az alkalmazható kártyák (Chipek) kiválasztását?
16. Vannak-e elõírt titkos kulcsú rejtjelezõ eljárások?
17. Dokumentálható-e ezek megbízhatósága, ha igen milyen idõtartamra dokumentálható?
18. A kulcsméretek megfelelnek-e a jelenleg elfogadottnak (RSA 1024 bit, ECC 135 bit)?
19. A kulcstárolásnál nehézségeket okozhat, ha a kulcsokat akár túl kevés, akár túl sok ember ismeri. Megoldást jelenthet az *(n,k)* küszöbrendszer alkalmazása. E rendszerek lényege, hogy a kulcsot *n* részre osztva, bármelyik k kulcsrészletbõl a kulcs elõállítható, de nincs olyan *k-1* kulcsrészlet, amibõl ez megtehetõ lenne.
20. Milyen a rejtjelezõ kulcs életciklusa?
21. Vizsgálták-e, dokumentálták-e, hogy egy adott alkalmazás szempontjából melyik kriptográfiai rendszer a jobb választás? Például a két leggyakrabban használt eljárás, az RSA és az ECC közül, a szakirodalom szerint nem dönthetõ el egyértelmûen jósági sorrend, csak adott alkalmazás szempontjából mondható meg, hogy melyiket célszerû használni.

22. Kriptográfiai protokollok vizsgálata, a legbiztonságosabb kriptográfiai algoritmusok esetén is szükség van olyan rendszabályokra, amelyek biztosítják, hogy az adott alkalmazásban ezek az algoritmusok a megkívánt titkosságot, vagy hitelességet nyújtsák. Az ilyen elõírások, rendszabályok összességét nevezik kriptográfiai protokollnak.

4.4. A hálózatok biztonsági kérdései

Az egyre nagyobb hálózatok számos elõnye mellett, a biztonságot érintõ kockázati tényezõk nagy mértékben növekedtek. Ez nem azt jelenti, hogy a jövõ az egyedi gépeké, de a megfelelõ biztonsági intézkedések nélkül létrehozott hálózati csatlakozás nem lebecsülendõ veszélyeket rejthet.

Ebben a fejezetben rendszer-összeomlásokkal, csalásokkal, nagyobb hibákkal, támadások vizsgálatával, számítógépes vírusokkal, férgekkel, trójai programokkal foglalkozom.

Számítógépes vírusnak nevezzük az olyan programtörzset, amely képes önmaga reprodukálására, figyelembe véve a mindig változó környezetet. *Logikai bomba* hatás révén egy beépített feltételhez kötötten (pl.: konkrét idõpont, szabad lemezterületi helyek száma, esemény bekövetkezése, logikai változó adott értéke stb.) *trójai faló* hatást indít el.

Az informatikai biztonsággal és a vírusokkal foglalkozó cégek tájékoztatását figyelve azt a következtetést lehet levonni, hogy a vírusok elleni védekezésben bizonyos szempontból elõnynek nevezhetõ, hogy az új számítógépes vírusok száma az összeshez viszonyítva kb. 20%. A megmaradó 80% vírusmutáció, amelyeket már létezõ programkód felhasználásával, átírásával vagy módosításával hoztak létre, így a védekezés ellenük valamivel egyszerûbb. Általában a vírusok elleni védekezést az nehezíti, hogy míg az 1980-as években az elsõ vírusok megjelenésekor 5-6 vírust ismertek, napjainkban pedig ennél havonta több mint a duplája jelenik meg.

A *férgek* a fertõzés mechanizmusában térnek el a vírusoktól, nem fertõznek meg minden programot, egyik programból vándorolnak a másikba.

A *trójai faló* olyan programtörzs, amelyet készítõje illegálisan épített be az általa tervezett programba és a felhasználó szándéka ellenére és tudta nélkül hajt végre illegális feladatokat (adattörlés, illegális lemezmûvelet, program megsemmisítés stb.).

Egy szervezet hálózatának biztonsága érdekében a gyakorlatban már bevált lépéseket lehet tenni, ilyenek például a következõk:

- Biztonsági intézkedések meghozatala, biztonsági terv kialakítása, amely során adminisztratív eszközökkel próbálják megvédeni hálózatot. Meghatározzák a védelem szempontjából fontos feladatokat, felelõsségi köröket (pl. a legfrissebb javítások telepítése, a szerverszobába való belépés rendje,…).

- Tûzfalak telepítése, nagyon sok ilyen termék létezik, ezeknek többféle típusa, tudása, lehetõsége van. A jól konfigurált, karbantartott tûzfal sok támadási kísérletet képes megállítani.
- A betörésvédelmi rendszerek alkalmazása.
- A védelmi rendszer telepítése után állandó ellenõrzésre, tesztelésre van szükség, különösen változtatások alkalmával (pl. új operációs rendszer bevezetése). Ez a tesztelés a hackerek teszteléséhez hasonlít, de megelõzi az õ tevékenységüket. A hálózaton, tûzfalakon, szerveren történõ eseményekrõl a gép naplókat készít, a naplókat állandóan elemezni, vizsgálni kell, így a támadásra utaló jelek felfedezhetõk.
- Egy olyan egység létrehozása, amelynek segítségével részletes jelentések nyerhetõk ki, melyek csaknem minden, a címtárral kapcsolatos eseményt rögzítenek. Felderíthetõ, mely felhasználók rendelkeznek adminisztrátori jogokkal és hogy szerepelnek-e az ACL-ben (az access control list-ben). Fény derül a jelszóváltozásokra és a sikertelen bejelentkezésekre az eDirectoryba. Létezik olyan termék, amely valós idejû riasztást ad behatolás érzékelésekor és naplóz is.
- Olyan védelmi rendszer kiépítése, amely nemcsak figyeli, hanem meg is akadályozza a behatolási kísérleteket a hálózati szerveren.
- Olyan védelmi rendszer kiépítése, amely az alhálózatok forgalmát figyeli, és gyanús eseményeknél figyelmezteti a hálózati szerver védelmét.
- A legújabb biztonsági frissítések nyomon követése.
- A legfrissebb vírusirtó szoftverek használata.

Az elemzés során az elõbbiek megvalósítását kell vizsgálni, ezeken kívül fel kell venni az informatikai hálózat naprakész térképét. Választ kell kapni, hogy ki férhet hozzá a különbözõ adatokhoz, felvetõdik a kémkedés, ipari kémkedés lehetõsége.

A számítógéprendszerek alapeleme a felhasználó azonosítása. Az azonosító tényezõ lehet jelszó, token[51], az ember valamely biológiai tulajdonsága. Ezeknek a tényezõknek a kombinálásával jött létre a többtényezõs azonosítás technikája, amely javítja az azonosítás megbízhatóságát. Sok helyen a jelszó az egyetlen azonosító eszköz. A felhasználók esetleg könnyen hozzáférhetõ helyeken tárolják a jelszavaikat (képernyõre ragasztott papírdarabon vagy mobiltelefonon). Ha a felhasználó bejelentkezés után elhagyja a gépét, akkor el kell érni, hogy bizonyos inaktív idõ után egy program lezárja a munkaállomást.

A munkaállomásokon is sok, esetleg bizalmas adatot lehet tárolni, ebben az esetben két kockázati tényezõ is felvetõdik, nem készül az adatokról biztonsági másolat, és az értékes információk a géppel együtt eltulajdoníthatók. Biztonságosabb, ha a valamilyen szempontból kiemelt adatokat kizárólag szervereken tárolják. A noteszgépek a

[51] token: gyûjtõfogalom, amely a hardveres személyi azonosító eszközöket jelenti (egyedi, valós tárgy). Leggyakrabban jelszóval vagy PIN-nel kombinálják. Számos típus létezik, például amelyik 30 másodpercenként új, hat jegyû kódot jelez ki. A felhasználónak ezt és egy PIN-t kell megadnia az autentikációhoz.

legkevésbé biztonságos adattárolónak számítanak. Átlagosan minden tizennegyedik ilyen mobil gépet ellopják[52] és legtöbbjükön védtelenek az adatok. Ha a noteszgép operációs rendszere megköveteli is a jelszó használatot, a tolvajnak vannak eszközei és van ideje is a gépen tárolt adatok megszerzésére, ezen kívül biztonsági másolat nélkül az adatok is elvesznek a géppel együtt. Az adatokon különbözõ adatmûveletek hajthatók végre (törlés, másolás, feldolgozás, tárolás, …). Hálózat esetén, védelmi intézkedések nélkül bárki ezeket a mûveleteket elvégezheti, ennek megakadályozására két elemi lehetõség van; vagy kizárják az elérésbõl azokat, akiknek nincs szükségük az adott információkra és/vagy titkosítjuk az adatforgalmat.

Hatékony módszer az adatok védelmére a rejtjelezés, a digitális aláírással pedig a dokumentum hitelességét lehet biztosítani.

Ha a felhasználók vagy ügyfelek az interneten keresztül érhetik el a belsõ erõforrásokat, akkor különleges intézkedések szükségesek. A védelem elsõ lépcsõfoka a tûzfal, de önmagában nem védi meg az egész hálózatot. A védelmi rendszerek, szolgáltatások és irányelvek összessége, amelynek része a behatolás-jelzõ rendszer, az autentikáció és annak felügyelete, auditáló és megfigyelõ eszközök, vírusok elleni védelem, valamint olyan irányelvek, amelyek elõsegítik a szabályok, a védelmi intézkedések betartatását. Az irányelveknek tartalmaznia kell, hogy mely részterületek lesznek elérhetõk, meg kell oldani a felhasználók azonosítását, esetleg titkosítani kell a szerverek közötti adatforgalmat.

A külsõ támadások vizsgálatánál, a kockázatelemzés egyik segítõje lehet az „ethical hacking” (etikus hackelés) eljárás. A hackelésbõl származó ismereteket jól képzett szakemberek vagy szakemberek csoportja a vizsgált szervezet érdekében tudja hasznosítani.

Az ethical hacking három jól elkülönítendõ fázisa;

- elõkészítõ fázis,
- támadási fázis,
- adminisztrációs fázis.

Az *elõkészítõ fázis* feladatai:

A jogalap megteremtése, mûszaki elõkészítés, katasztrófa-elhárítási terv készítése, az adatok mentése. Az elõkészítés közös feladata a megrendelõnek és a vizsgálatot végzõnek.

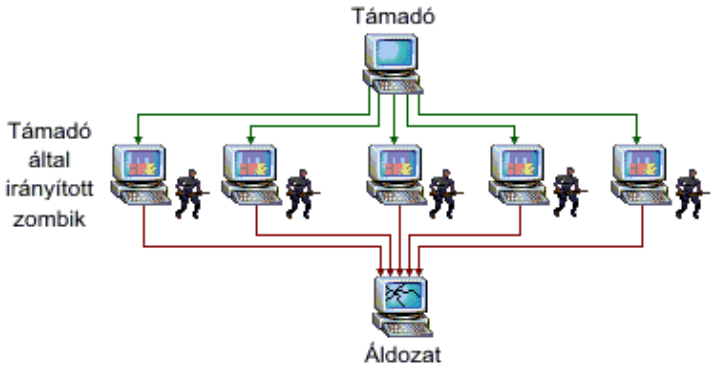
A *támadási fázis* feladatai;

- a hálózati forgalom elemzése,
- vírus-teszt,
- jelszó-megfejtés,
- hamisított levél küldése,
- információszerzés az adott szervezetben,
- hordozható számítógéprõl adatszerzés,

[52] Forrás: Novell ConNection, A hálózati szakértõk magazinja, 2002. január.

- web-, levelezõszerver sérülékenységének a kihasználása,
- buffer overflow (a programok rossz input kezelését kihasználó feltörési technika),
- DDoS támadás,

  A hálózat-alapú DDoS (Distributed Denial of Service) típusú támadás lefoglalja a támadott gép hálózati sávját és a legrosszabb esetben a rendszer teljes összeomlásához is vezethet.



4.1. ábra. Az elosztott túlterheléses támadás lényege
Illusztráció: Symantec[53]

A támadók általában nem saját gépeik, hanem trójai programokkal vagy férgekkel feltört, valójában más emberek által üzemeltetett ún. zombik segítségével támadnak, ami gyakorlatilag lehetetlenné teszi a valódi és a csak a túlterhelés céljával küldött kérések megkülönböztetését. Ebben az esetben általában a támadók azonosítása is nehezebb.

- modem pool támadás.

  A modem pool olyan, mintha egyetlen eszközbe vonták volna össze egy szervezet összes modemjét. A felhasználók kimehetnek az Internetre vagy igénybe vehetnek on-line szolgáltatásokat anélkül, hogy minden munkaállomás mellé egy modemet kellene telepíteni.

A *adminisztrációs fázis* feladata egy olyan dokumentum készítése, amely tartalmazza a

- az információ-szerzés eredményét,
- a támadások listáját és eredményét,
- a talált sérülékenységek összefoglalását,
- megoldási javaslatokat.

A kockázatelemzés egy elképzelt hacker-betörés alapján végezhetõ:

A hacker lépései:	**A mérlegelés szempontjai:**
1. információgyûjtés A hacker az adott szervezet honlapjáról a dolgozók, a rendszergazdák nevét, kapcsolataikat, esetleg fogyasztónak, felhasználónak, érdeklõdõnek kiadva magát e-mailen telefonon keresztül, a WHOIS és DNS szerverrõl nagyon sok számára lényeges információt tudhat meg.	Az adott szervezet érdekeit mi szolgálja jobban, a teljes vagy részleges ismertetés önmagáról egy Web oldalon vagy a teljes, esetleg részleges hírzárlat. Érdeklõdõknek, fogyasztónak, megrendelõnek milyen információ adható.

[53] Symantec: A Symantec Corp. internetes biztonságtechnikával foglalkozó vállalat.

2. a hálózat letapogatása - A hacker pingeli vagy szkeneli a portokat. A port scan és a ping sweeps megmutatják, melyek az élõ és elérhetõ TCP porttal rendelkezõ gépek és rendszerek. - A következõ szkenelés az egyedi gyenge pontok megkeresésére irányul. Például, a hacker képes információt szerezni az FTP szervertõl arról, hogy milyen szoftver fut rajta. - A régebbi szoftverek jól ismert gyenge pontokkal segítik a hacker munkáját. Megjegyzés: Az elsõ két lépésben a hacker még nem követett el büntetendõ cselekményt.	- Az elterjedtebb FTP szerver programok jelentõs részének kódja nem auditált, így tartalmazhat buffer overflow-t, így használatuk kockázatos lehet (pl. proftpd, wu-ftpd). - A szervezetnek megéri-e mindig a legújabb programokat, szûrõket, a weboldalak és az FTP oldalak ellen irányuló támadásokkal szembeni védelmet kiépíteni vagy megvásárolni ezeknek a hibáknak a kiküszöbölésére? - A régebbi szoftverek elleni támadás kivédhetõ, ha a rendszert a legújabb szerviz csomagokkal és javításokkal naprakésszé teszik.
3. betörés a hálózatba - a szerveren levõ hibák kihasználása, - jogosultságok megszerzése, - biztonsági rések megtalálása az eddigi információk alapján, - tûzfal feltörés.	Átfogó biztonsági intézkedések megtervezése, amelyek követendõ szabályokat írnak elõ a szervezet részére. Ez az intézkedés csomag tartalmazza a felhasználói jelszavak és a hozzáférési jogok szabályozását is.
4. tárcsázó kapcsolatok problémája A tárcsázó kapcsolatok jelentik a legkönnyebben támadható felületeket. Gyakran engedélyeznek a felhasználóknak a belsõ rendszerhez való közvetlen hozzáférést tûzfal és proxy nélkül. A hacker meg tudja szerezni a tárcsázó kapcsolat számait és így át tudja küldeni õket más modemekre.	- A tárcsázási kapcsolatok ritkán naplózzák a tevékenységet, így tökéletes alkalmat adnak a betörésre. Meggondolandó a naplózás bevezetése.

<table>
<tr><td>5. a távmunkát végzõk problémája
Azok a dolgozók, akiknek tárcsázó, DSL[54], vagy ISDN[55] kapcsolatuk van otthon, különösen ki vannak téve a támadás veszélyének. A hacker be tud törni az otthoni számítógépükbe, ami sokszor sokkal könnyebb, mint bejutni egy vállalat szerverébe. Ha a hacker bejutott az otthoni gépbe, bejuttat egy férget vagy vírust, amely megfertõzi a vállalati hálózatot, amikor a távmunkát végzõ rákapcsolódik. A vírus képes arra, hogy rést üssön a Tûzfalon, így a hacker bejut a vállalat hálózatába.</td><td rowspan="2">- Egy jól konfigurált, folyamatosan karban tartott, rendszeresen tesztelt tûzfal sok támadástól megvéd. El kell dönteni, hogy a védendõk egyensúlyban vannak-e az ilyen tûzfal üzemeltetésével.
- A tûzfal nem mindig elégséges, ha a védendõk nagyobb értéket képviselnek, akkor a hálózatnak átfogó betörésvédelmi rendszerre van szüksége. Egy mindenre kiterjedõ betörésvédelmi rendszer a hálózat minden egyes pontját figyeli. Minden munkaállomás, minden szerver, minden router védelem alatt fog állni azoknak az alkalmazottaknak az otthoni gépei is, akik otthonról be tudnak lépni a rendszerbe. Így még a rendkívül sebezhetõ tárcsázó kapcsolattal rendelkezõ dolgozók is meg tudják védeni a hálózatot a betörésekkel szemben.
- A jelentések, illetve elemzések révén a rendszergazda a pingeléseket és port scan-eket idõben észlelheti, még mielõtt a hacker be tudna törni a rendszerbe. Sõt, mivel a központi bkáció folyamatosan kapja a jelentéseket a rendszerrõl, még a kevésbé védett távoli oldalak is képesek a tágabb értelemben vett hálózati védelem beindítására, ahelyett, hogy újabb lehetõségeket adnának a betörésre.</td></tr>
<tr><td>6. megosztott hálózatok problémája
A megosztott hálózatok számos kiskaput nyitnak a hackerek elõtt. Ha az egyik részhálózatnak nem elég jó a betörésvédelme, a részhálózatok összekapcsolódása után, a teljes hálózat biztonsága a kisebb biztonságú részhálózatéval egyezik meg.</td></tr>
<tr><td colspan="2">7. emberi gyengeségek kihasználása
- Sértõdött, elégedetlen, vagy éppen elbocsátott dolgozók, rendszergazdák, biztonsági szakemberek névtelenül nyilvánosságra hozhatnak minden adminisztratív jelszót egy levelezési csoportban vagy felhívhatják a figyelmet a biztonsági résekre.
- Ha a távozók kiskapuikat, vagy hozzáférési kódjaikat adják hozzá a rendszerhez, miután otthagyják a céget, az érvényes, még le nem tiltott jelszavukkal egyszerûen átmennek a tûzfalon, így már õk is hackernek számítanak.</td></tr>
</table>

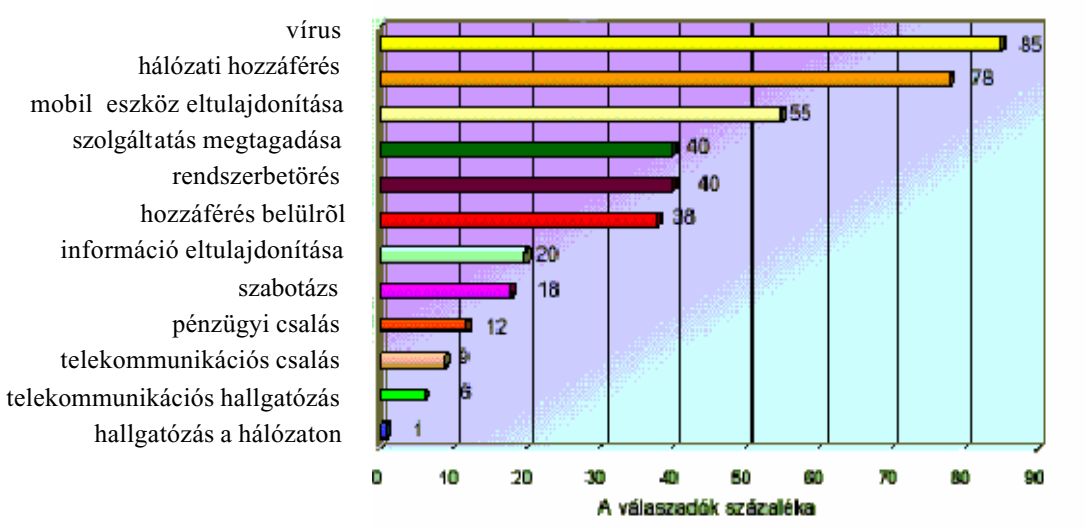
[54] DSL: Digital Subscriber Line. Ezek a kapcsolatok többnyire állandóak, a gépek gyakran statikus IP címet kapnak a szolgáltatótól; amíg a gép be van kapcsolva, addig az internet-kapcsolat is létezik és az IP címe is változatlan. Megfelelõ biztonsági beállítások nélkül bárki, aki erre a címre rátalál, elvileg belelát a gépbe.

[55] ISDN: Integrated Services Digital Network, Integrált Szolgálatú Digitális Hálózat. Az ISDN vonal több szolgáltatás (hang, kép, adat stb.) egy közös digitális csatornán való átvitelét biztosítja.

Minden szervezetnél el kell dönteni az informatikai rendszerben kezelt adatok és információk, szoftverek értékét, a rendelkezésre állás mértékét.

Az informatikai rendszer fenyegetettségét *statisztikai adatok és a szervezetben már elõfordult támadások alapján lehet meghatározni.* Figyelembe vehetõ például a következõ felmérés is.

A CSI/FBI FELMÉRÉSE A TÁMADÁSOKRÓL: (Forrás: CSI/FBI 2002 Computer Crirne and Security Survey Computer Security Institute)



4.2. ábra. Felmérés a támadásokról

A CSI és az FBI 2002-es jelentése szerint a megkérdezett nagyvállalatok 90%-ánál volt probléma az informatikai rendszerének biztonságával, 80%-a elismerte, hogy a rendszerében lezajlott hacker tevékenység anyagi kárral járt, a pontos összegeket is bevallóknál a kár több mint 455 millió dollár, a felmérésben résztvevõk 40%-a tapasztalt külsõ támadást az informatikai rendszere ellen.

Az internetre csatlakozó gépeknél a biztonságot fenyegetõ tényezõk nagyobbak, de van olyan szolgáltatás, amelynek segítségével megállapítható, hogy pillanatnyilag milyen szintû fenyegetettség áll fenn (pl. az Internet Security Systems bejelentette, hogy a Network Computing webhelyen át elérhetõ az ISS AlertCon szolgáltatása a pillanatnyi fenyegetettségrõl az interneten.).

Az Internet Security Systems egytõl négyig terjedõ skálán osztályozza naponta az aktív internetes fenyegetettséget.

1. szint: Hétköznapi tevékenységek folynak, amelyek az internet-kapcsolat létrejöttétõl számított több percen vagy órán belül eredményezik csak azt, hogy sérelem érje a védtelen hálózatokat. Szokásos éberség
2. szint: A számítógépes hálózatok sebezhetõ pontjai és fenyegetettsége a kockázat felmérésére és óvintézkedésekre adnak okot. Fokozott éberség

3. szint: Konkrét biztonsági rések állnak fenn, és támadható pontokra irányuló internetes támadások vannak folyamatban, amelyek haladéktalan védelmi intézkedéseket tesznek szükségessé. Célzott támadások
4. szint: A biztonsági helyzet kritikus, ezért a hálózaton belül haladéktalan és célzott védelmi intézkedéseket kell végrehajtani. Ez az állapot lehet küszöbön álló, illetve folyamatban lévõ. Katasztrofális fenyegetettség (Pl. ilyen fenyegetettség volt a Code Red féregvírus 2001. júliusában és a „SQL Slammer" féreg 2003 januárjában).

A lehetséges támadások és az értékek figyelembevételével döntést kell hozni a bevezetendõ intézkedésekrõl, törekedni kell a mindenütt hasonló szintû megoldásokra, az egyenszilárd biztonság kialakítására, mert ha egy hely is sebezhetõ, ezáltal az egész rendszer is támadhatóvá válik..

4.5. Kulcsfontosságú informatikai rendszerek állandó elérhetõségének biztosítása

Az állandó elérhetõséghez nagyon sok minden tartozik; az építõelemek megbízhatósága (ez nyilvánvalóan befolyásolja a hibák és leállások kivédhetõségét), a hibák, leállások gyors felismerése, az összegyûjtött adatokat kiértékelõ berendezések, olyan átviteli eszközök, melyek a helyreállításhoz, illetve az egyéb intézkedésekhez szükséges információkat továbbítják.

A *szerverek* mûködtetik az adatbázisokat, az alkalmazásokat, a szoftvereket. Így egy szerver kiesése negatív irányba befolyásolja a megbízhatóságot, a megoldást a szorosan szinkronizált, redundáns[56] konfigurációba rendezett szerverek adják, amelyek teljes másolatot készíthetnek egymásról. Itt fontos szerepet kap a hardveres hibafelderítés, illetve azok a felügyeleti eszközök, melyek lekapcsolják, kicserélik a meghibásodott elemeket, illetve kijavítják a rendszert.

A *tároló berendezések* megfelelõ használhatóságához minden hálózatban többszörös utaknak kell lenni, a hálózatnak biztosítania kell az izolációt, és a megbízható eszközöket a hibák felderítéséhez és kijavításához.

Adatbázisok felépítésének három típusáról beszélhetünk;

- a „minden közös" (Shared Everything), architektúrájú adatbázis nagyon sérülékeny, mert az adatbázis-kezelõ ugyanazon számítógép memóriájában fut, mint amelyiknek a lemezén az adatbázis tárolódik. A sérülékenység csökkentésére szinte az összes adatbázis mindenre kiterjedõ naplózást, illetve az adatbázis korábbi állapotának visszaállítására biztonsági mentés/visszaállítás funkciókat használ.

[56] redundáns: az elvileg elegendõ minimumon felüli többlet. Magyar Értelmezõ Kéziszótár.
Redundáns rendszerek: Ha meghibásodik valamelyik alkotóelem egy ilyen rendszerben, mindig van olyan tartalékelem, amely - lehetõleg automatikusan - át tudja venni a meghibásodott funkcióját.

- a „semmi sem közös” (Shared Nothing) architektúrában az *A* adatbázis naplójának átvétele révén a *B* adatbázis „visszaállhat” az *A* adatbázis naplózott állapotába, ha *A* meghibásodik.
- az „adat közös” (Shared Data) architektúrában a tároló egyetlen logikai lemeznek látszik, ahol az adatbázis több másolatát és a gyakorlatilag közös naplót tárolják. Ha az elsõ számú adatbázis leáll, bármelyik másolat átveheti annak a szerepét.

Az *alkalmazások* megbízható mûködéséhez mind az alkalmazást, mind a telepítés menetét jól kell ismerni. A szoftverleállások kezelésére egyre több megoldást alkalmaznak, a megfelelõ elérhetõség biztosításához hatékony tervezés, rendszeres munkafolyamatok és jól képzett dolgozók is szükségesek.

4.6. A fenyegetõ tényezõk rendszerezése

A harmadik fejezetben, a kockázatelemzési módszertan részeként (3.2.2.) azonosítottam az informatikai rendszer lehetséges gyenge pontjait. A kockázatelemzési eljárás sikere nagy mértékben függ a fenyegetõ tényezõk minél teljesebb körû feltárásától, annak érdekében hogy ez a számbavétel ne legyen hiányos a fenyegetõ tényezõket *humán, logikai, fizikai és környezeti tényezõk csoportjába rendszereztem*.

A negyedik fejezetben, az informatikai rendszer egyes részterületeinek elemzésénél kiemeltem azokat a veszélyes pontokat, helyzeteket, amelyeket az adott területen vizsgálni kell. *A fenyegetõ tényezõk rendszerezése egy-egy kiemelt részterület szerint is lehetséges.*

A harmadik és negyedik fejezetben leírt rendszerezéseken túl, elõsegítheti a veszélyelemzést a veszélyeztetõ faktorok katalógusának felépítése. Ebbõl kiindulva a következõkben a fenyegetõ tényezõk rendszerét mutatom be, öt szempont szerinti osztályozásban, ez a csoportosítás a felelõsség kérdését is sugallja.

FENYEGETÕ TÉNYEZÕK:

A. szervezési hiányosságokból adódó veszélyek,
B. technikai hiányosságok tényezõi,
C. emberi tényezõk,
D. szándékos cselekmények,
E. vis maior (magasabb kényszer) tényezõk.

Szervezési hiányosságokból adódó fenyegetõ tényezõk;

- hiányzó vagy nem megfelelõ rendelkezések ill. szabályok,
- a fennálló szabályok nem megfelelõ ismerete,
- hiányzó vagy nem alkalmas eszközök,
- az informatikai rendszer nem megfelelõ ellenõrzése,
- hiányos vagy nem megfelelõ karbantartás,
- illetéktelenek belépése a védendõ helyiségekbe,
- rossz munkakörülmények,
- nem megfelelõ vezetékkapacitás,

- a védett adatok bizalmasságának elvesztése,
- az adathordozók hiányos jelölése,
- a rejtjelezés nem megfelelõ kulcskezelése,
- jegyzõkönyvek adatainak hiányzó kiértékelése,
- nem megfelelõ teszt és átadás-átvételi eljárások,
- hiányzó vagy hiányos dokumentációk (gépkönyvek, kezelési utasítások, megvalósulási tervek, mûbizonylatok, jegyzõkönyvek stb.),
- szoftverteszt valódi adatokkal,
- a szerverek nem biztonságos elhelyezése,
- a biztonsági rendszer hiányos, nem megfelelõen aktivált,
- a felhasználói környezet kialakítása nem megfelelõ,
- a szervezet szolgáltatói környezetének kialakítása nem megfelelõ,
- a már meglévõ technikai rendszerhez történõ nem megfelelõ csatlakozás,
- rendezetlen felhasználóváltás a munkaállomásokon,
- a kommunikációs összeköttetés nem ellenõrzött,
- a hálózat és a szerverstruktúra tervezésének gyenge pontjai,
- nem biztonságos adathordozó szállítás és tárolás,
- a rendszergazdák és munkatársak nem megfelelõ képzettsége,
- rendezetlen e-mail használat stb.

Technikai hiányosságokból adódó fenyegetõ tényezõk;

- áramellátás kiesése, feszültségingadozás,
- az intranet hálózat kiesése,
- a biztonsági berendezések meghibásodása,
- hibás adathordozók,
- a hitelesítési lehetõség hiánya a szerver és a munkaállomás között,
- tárolt adatok elvesztése,
- rossz címre történõ adatküldés, pl. kapcsolási hiba miatt,
- adatátviteli hiba,
- adatvesztés a nem megfelelõ tárolókapacitás miatt,
- a rendszerszoftver gyenge pontjai,
- az adatbank egészének, egy részének vagy integritásának elvesztése,
- az informatikai rendszer egyes egységeinek meghibásodása stb.

Emberi, nem szándékos károkozás fenyegetõ tényezõi;

- biztonsági intézkedések figyelmen kívül hagyása,
- tévesztésbõl eredõ, nem szándékos károkozás,
- a takarító, a karbantartó személyzet nem szándékos károkozása,
- a IT rendszer nem megfelelõ használata,
- hibás vagy rossz adatok bevitele, ill. átvitele,
- a belépési jogok hibás adminisztrációja,
- az IT rendszer nem engedélyezett, saját célra történõ használata,

- az adattárolás szervezetlensége stb.

Szándékos cselekmények;

- az IT eszközök (adatok, hardver, szoftver, vezetékek stb.) károsítása,
- illetéktelen behatolás az épületbe, lopás, vandalizmus, merénylet, lehallgatás,
- jogosulatlan, rossz szándékú IT használat,
- karbantartáskor megszerzett információk alapján történõ visszaélés,
- külsõ vagy belsõ személy általi veszélyeztetés a karbantartási munkáknál,
- jelszó megtalálására irányuló tevékenység,
- visszaélés a használói, az adminisztrátori jogokkal,
- számítógép vírusok, trójai faló stb.,
- adatok jogosulatlan másolása,
- behatolás a számítógépes rendszerbe,
- az adatátvitelnél történõ visszaélés, vonallehallgatás,
- kényelmi szempontból a védelmi intézkedések szándékos kikerülése,
- illetéktelen hálózatkezelési eljárások véghezvitele,
- hálózati komponensek nem jogos használata, visszaélés az e-mail használattal stb.

Vis maior tényezõk:

- villámcsapás, tûz, árvíz,
- por, levegõszennyezettség,
- adatvesztés erõs mágneses mezõ miatt,
- magas hõmérséklet, levegõ páratartalom,
- harci cselekmény, IT rendszer, belsõ hálózatok támadása stb.

Az értekezésem egyik kitûzött célja volt az informatikai biztonságot fenyegetõ tényezõk több részletre kiterjedõ feltárása és rendszerezése. Az elvégzett feladatot ebben a fejezetben foglaltam össze.

4.7. Összegzés

Az összegzés során felvetõdik a kérdés, hogy az informatikai rendszerek kockázatelemzésének minden problémája felmerült ebben a fejezetben? Nem. A valóság sokkal gazdagabb, mint bármilyen elmélet.

Az általam a védelmi szférában kiemelten fontosnak tartott kérdéskörrel foglalkoztam. Így a fizikai környezet, a környezeti infrastruktúra sajátosságait, az informatikai alkalmazások, a rejtjelezés kockázatelemzését, a hálózatok biztonsági kérdéseit, a kulcsfontosságú informatikai rendszerek állandó elérhetõségének problémakörét részesítettem elõnybe.

A gyakorlatban az informatikai rendszer egyes részterületei összetartoznak, átfedhetik egymást. A szervezeteknek biztonságuk érdekében tisztában kell lenniük informatikai rendszereik lényeges részterületével azok gyenge pontjaival, kockázataival, valamint azzal, hogy miként és milyen biztonsági intézkedésekkel tudják mérsékelni ezeket.

5. Az eredmények összegzése, az értekezés felhasználhatósága

A dolgozat zárófejezetében a kutatás alapvetõ céljait, az elért eredményeket és azok hasznosíthatóságát foglalom össze, valamint azokat a területeket érintem, amelyek még új kutatási irányokat jelenthetnek.

A bevezetõben megfogalmazott célkitûzések elérése érdekében;

- **Meghatároztam** azokat az alapfogalmakat, amelyeket az értekezésemben használtam, **áttekintettem** az informatikai biztonság kialakítása során figyelembe veendõ jogszabályokat, szabványokat és ajánlásokat, **rendszereztem** a biztonsági osztályokra vonatkozó egységes követelményeket.
- A védelmi szféra érdekeinek figyelembevételével **kiválasztottam** különbözõ kockázatelemzõ módszereket, amelyeknek a pozitívumait és negatívumait **vizsgáltam**, felállítottam egy összehasonlítási szempontrendszert és ennek segítségével **értékeltem** és **összehasonlítottam** a kiválasztott eljárásokat, az összehasonlítás eredményeit grafikonon szemléltettem.
- **Elemeztem** és **összehasonlítottam** a két leggyakoribb veszélyelemzõ módszer (a hibafa és eseményfa) megvalósíthatóságát. **Összegeztem** az informatikai rendszerek teljes életciklusán végigvezetõ veszélyelemzési folyamatokat.
- **Kidolgoztam** egy kockázatelemzési módszertani útmutatót a védelmi szféra informatikai rendszereinek kockázatelemzésére. **Kialakítottam** az informatikai biztonságot fenyegetõ tényezõk rendszerét.
- **Kiemeltem** az informatikai rendszer egyes részterületeit, **ráirányítottam a figyelmet** az adott részterület biztonsági vizsgálatának releváns tényezõire.

Mindezek alapján az informatikai rendszerek biztonságának kutatása során elért **tudományos értékû eredménynek tekintem**

1. **A kiválasztott kockázatelemzési módszertanok** (Cobit, CRAMM, ITB 8. számú ajánlás, MARION, IT-Grundschutzhandbuch) **összehasonlító elemzését.**

2. **A védelmi szféra informatikai rendszereinek kockázatelemzésére kidolgozott kockázatelemzési módszertant.**

3. **Az informatikai biztonságot fenyegetõ tényezõk rendszerének kialakítását.**

A téma kidolgozásával hozzá kívántam járulni;

- az informatikai biztonság kérdéskörének elméleti és gyakorlati továbbfejlesztéséhez,
- a felsõfokú oktatásban használható informatikai védelmi infrastruktúrák továbbfejlesztéséhez,
- az informatikai rendszereket fenyegetõ támadások felismeréséhez, mivel ez a felismerés az elsõ lépése a sikeres biztonsági rendszer kialakításának.

Az értekezésem felhasználását javaslom:

- A kialakítás alatt álló válság- és konfliktuskezelés oktató és kutató központ informatikai rendszerének biztonsági elemzésénél.
- A válság- és konfliktuskezelés oktató és kutató központ oktatási segédleteinek kidolgozásánál.
- Az informatikai rendszereket fenyegetõ tényezõk figyelemmel kísérésénél, ami segíti a veszélyhelyzetek megelõzését.
- Az általános módszertan a védelmi szféra informatikai rendszereinek kockázatkezelésénél közvetlenül vagy a változások figyelemmel kísérésével kisebb módosításokkal alkalmazható.
- Az eredményeim nemcsak a védelmi szféra mûködési területén hasznosíthatók, hanem pl. banki, kormányzati területeken is támogatják a felhasználót.
- A felsõfokú oktatásban, a kutatómunkában közvetlenül hasznosíthatók az összehasonlító elemzések (2.2. fejezet).
- A kidolgozott veszélyelemzési módszerek alkalmazhatók megelõzési célból, a védelmi szféra informatikai rendszereit fenyegetõ veszélyek vizsgálatában.

A további kutatások iránya:

- Vizsgálat tárgyát képezheti az informatikai rendszerek fejlõdésének hatása a biztonságra.
- A szervezetek az informatikai rendszereik elleni támadások nagy részét nem publikálják, mivel ez károsan befolyásolhatja a szervezet hírnevét. Kutatási terület lehet a számítógépes bûncselekmények vizsgálata és azok elõfordulási valószínûségének és irányának becslése.
- Az informatikai rendszerek biztonságának kockázatelemzése egy elfogadott szükségszerûség, ennek ellenére a szervezetek a már elért eredmények nyilvánosságra hozását akadályozzák és minõsített információként kezelik, ami bizonyos szempontból érthetõnek is tekinthetõ. Vizsgálható, ennek az ellentétes hatásnak a feloldása.

Irodalomjegyzék

Hivatkozott irodalom:

[1] Muha Lajos: Az informatikai biztonság kézikönyve, VERLAG DASHÖFER Szakkiadó Kft.& T.Bt., Budapest, 2002. 3.2. fejezet, p. 3.-5.

[2] Ködmön József: Kriptográfia, COMPUTERBOOKS, Budapest, 1999/2000. p.65-66.

[3] Váncsa Julianna: Az informatikai biztonság alapjai, ZMNE. Egyetemi jegyzet, Budapest, 2000. p.7.

[4] Mûszaki Biztonsági Fõfelügyelet: 'Seveso 2' Füzetek, 3. sz. Füzet Technológiai rendszerek kockázatelemzése, MBF. Budapest, 2001. p. 19.

[5] NATO Defense Capabilities Initiative, Press Release NAC-S(99)69, 25 April 1999. NATO Security Policy C-M(2002)49.

[6] http://archiv.tu-chemnitz.de/pub/2002/0105/data/services/eta.htm

[7] Szabó Géza: Nagy biztonságú rendszerek megbízhatósági analízise és közlekedési alkalmazásai. PhD disszertáció. BME Közlekedésautomatikai Tanszék, 2001.

[8] Mezey Gyula: Biztonságos információrendszerrõl vezetõknek, OMIKK, Bp, 1997. p.22-30.

[9] http://www.kum.hu/euanyag/eumagyar2001/bel-ig7.htm

[10] Dr. Szakács Ágnes: A környezeti funkció szerepe a honvédségnél a békefelkészítés változó környezeti kockázatának függvényében http://www.zmka.hu/tanszekek/vegyi/docs/fiatkut/Dr1agi.htm

[11] Guide to the NATO Science Programme, Scientific Affairs Division NATO, Brussels, 2000. (23. p)

[12] NATO Guide for the Delegation of Government Quality Assurance, (AQAP-170). NATO International Staff-Defence Support Division, 1997. ANNEX C-1.

[13] Borgulya István: Neurális hálók és fuzzy rendszerek, Dialóg Campus Kiadó, 1998, p.104-113.

[14] http://infosrv.tech.klte.hu/~pokoradi/tezis_fuzet.pdf, dr. Pokorádi László: Döntés elõkészítési módszerek a repülõgépek üzemeltetésében, Habilitációs tézisek, 2002.

[15] Bárdossy György: A földtani kutatás bizonytalanságai és kockázatai, új utak ezek megoldására, Magyar Tudomány, 2002/9, p. 1227-1234.

[16] Soós László: Üzembiztonság, szünetmentes áramellátás, CEM Oktatási segédanyag kivonata, Budapest, 2003, (http://www.enga.hu/conference/ea02.pdf)

Felhasznált irodalom:

1. Crume, Jeff: Az internetes biztonság belülrõl : ...amit a hekkerek titkolnak, Szak Kiadó Kft., 2003.
2. Dietz Gusztávné Dr. Pap Márta: Adatvédelem, adatbiztonság, NOVORG, Bp., 1995.
3. F. Ható Katalin: Adatbiztonság, adatvédelem, SZÁMALK Kiadó, 2000.
4. Hadtudományi Lexikon, Magyar Hadtudományi Társaság, Bp., 1995.
5. Dr. Kovács Magda: Mikroszámítógép-mikroelektronikai értelmezõ szótár, LSI Alkalmazástechnikai Tanácsadó Szolgálat, Bp., 1989.
6. Ködmön József: Kriptográfia, COMPUTERBOOKS, Bp., 1999/2000.
7. Kun István: Gazdasági statisztika, LSI, Bp, 1998.
8. Dr. Kun István, Dr. Szász Gábor, Dr. Zsigmond Gyula: Minõség és megbízhatóság, LSI, Bp., 2002.
9. Martin, James: Security, accuracy and privacy in computer systems. http://wigwam.sztaki.hu/rfc/?2291
10. MSZ EN ISO 9000:2001 Minõségirányítási rendszerek. Alapok és szótár.
11. MSZ EN ISO 9001:2001 Minõségirányítási rendszerek. Követelmények.
12. MSZ EN ISO 9004:2001 Minõségirányítási rendszerek. Útmutató a mûködés fejlesztéséhez. Szabványügyi Hivatal, Bp., 2001.
13. Muha Lajos: Az informatikai biztonság kézikönyve, VERLAG DASHÖFER Szakkiadó Kft.& T.Bt., Bp., 2002.
14. Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, PRO-SEC Kft., Bp., 2001.
15. Munk Sándor: Az információs mûveletek típusai és modelljei, Hadtudomány, 2002/1.
16. Mûszaki Biztonsági Fõfelügyelet: 'Seveso 2' Füzetek, 3. sz. Füzet Technológiai rendszerek kockázatelemzése, MBF. Bp., 2001.
17. Norton, P.-Stockman, M.: A hálózati biztonság alapjairól. Kiskapu Kft, 2000.
18. Obádovics J. Gyula: Valószínûségszámítás és matematikai statisztika, SCOLAR Kiadó, Bp., 1995.
19. Schutzbach Mártonné: A számítógépek fejlõdésének hatása az RSA titkosítási eljárásra, KARD ÉS TOLL, 2002/2, 134 p.
20. Schutzbach Mártonné: Az informatikai biztonság általános koncepciója és gyakorlata a védelmi szférában, Nemzetvédelmi Egyetemi Közlemények, 5. évfolyam, 4. szám, 2001, 132 p.
21. Schutzbach Mártonné: Az informatikai biztonságot fenyegetõ tényezõk, Nemzetvédelmi Egyetemi Közlemények, 7. évfolyam, 2. szám, 2003, 155 p.
22. Schutzbach Mártonné –Dr. Kun István: Matematikai modellek az adattitkosításban, Informatika folyóirat, 4. évfolyam, 3. szám, 2001. november, 42 p.
23. Schutzbach Mártonné: Kockázatelemzési módszerek áttekintése, KARD ÉS TOLL, 2003/1, 195 p.

24. Szvetnik Natália: Elõzetes kockázatbecslési eljárások módszertani elvei és sajátosságai a nemzetközi gyakorlat tükrében, Környezetvédelmi Minisztérium, 2001.
25. Tóth Tibor: Minõségmenedzsment és informatika, Mûszaki könyvkiadó, Bp., 1999.
26. Turcsányi Károly –Vasvári Ferenc: A biztonságtudományról és szerepérõl a korszerû menedzserszemlélet kialakításában, Hadtudomány, 1999. 1. szám, 99 p.
27. Dr. Vasvári Ferenc: A haditechnikai menedzsment reálfolyamatainak kockázatértékelési és kockázatkezelési módszerei, PhD értekezés, ZMNE, 2002.
28. Zsigovits László: A határõrség informatikai rendszere fejlesztésének lehetõségei és feladatai, PhD értekezés, ZMNE, 2001.
29. Dr. Zsigovits László: A bevetés irányítás információtechnológiája és eszközei, Egyetemi jegyzet, ZMNE, 2003.

Internet felhasználások:

1. http://archiv.tu-chemnitz.de/pub/2002/0105/data/services/fta.htm
Thomas Müller: Dienste: Zuverlässigkeit, Verfügbarkeit und Ausfallrisiken.

2. http://infosrv.tech.klte.hu/~pokoradi/tezis_fuzet.pdf Döntés-elõkészítési módszerek a repülõgépek üzemeltetésében, Habilitációs tézisek, Benyújtva a Budapesti Mûszaki és Gazdaságtudományi Egyetem Közlekedésmérnöki Karához, dr. Pokorádi László a mûszaki tudomány kandidátusa fõiskolai tanár, 2002. április.

3. http://www.itb.hu. Informatikai Tárcaközi Bizottság honlapja

4. http://www.isaca.ch Az ISACA svájci honlapja.

5. http://www.kka.bme.hu/~kozlaut/Szubmodul/SAFETY-CRITICAL%20COMPUTER%20SYSTEMS.pdf
Biztonságkritikus számítógép rendszerek. BME, Közlekedésautomatikai Tanszék, 2002.

6. http://www.mbh.hu Kockázatértékelés a BS 8800:1996 angol szabvány tájékoztatója alapján.

7. www.munkavedelem.hu
OMMF (Országos Munkabiztonsági és Munkaügyi Fõfelügyelõség) Útmutatás a munkahelyi kockázatértékeléshez.

8. http://www.ntru.com NTRU Cryptosystems.

9. http://www-5.ibm.com/hu/services/its/security.pdf IBM Security and Privacy Services, Enabling and protecting e-business.

10. http://www.profes.hu PROFES+3. Kockázatmenedzsment támogató rendszer.

11. http://www.szgti.bmf.hu/~mtoth/download/Kriptografia/Szimmetrikus/SzimmetrikusKriptorendszerek.pdf Szimmetrikus kriptorendszerek, Randall K. Nichols: ICSA (ICSA: International Computer Security Association), Guide to Cryptography c. könyve alapján interpretálta Dr. Tóth Mihály

12. http://tldp.fsf.hu/HOWTO/Apache-WebDAV-LDAP-HOWTO-hu/ssl.html Az SSL megvalósítása és használata a HTTP forgalom biztonságossá tételére.

Publikációs jegyzék

- Schutzbach Mártonné: A számítógépek fejlõdésének hatása az RSA titkosítási eljárásra, KARD ÉS TOLL, 2002/2, 134 p.

- Schutzbach Mártonné: Az informatikai biztonság általános koncepciója és gyakorlata a védelmi szférában, Nemzetvédelmi Egyetemi Közlemények, 5. évfolyam, 4. szám, 2001, 132 p.

- Schutzbach Mártonné: Az informatikai biztonságot fenyegetõ tényezõk, Nemzetvédelmi Egyetemi Közlemények, 7. évfolyam, 2. szám, 2003, 155 p.

- Schutzbach Mártonné –Dr. Kun István: Matematikai modellek az adattitkosításban, Informatika folyóirat, 4. évfolyam, 3. szám, 2001. november, 42 p.

- Schutzbach Mártonné: Kockázatelemzési módszerek áttekintése, KARD ÉS TOLL, 2003/1, 195 p.

- Elisabeth Schutzbach: Risikoanalyse: Aufdeckung von Schwachstellen und Risikofaktoren, BOLYAI SZEMLE, 2002. 4. szám, 127 p.

- Schutzbach Mártonné: Matematikai modellek és módszerek a védelmi informatikában, az adattitkosítás kockázatelemzése a védelmi informatikában, NEMZETVÉDELMI EGYETEMI DOKTORANDORUM, 2002. 2. szám, 197 p.

- Schutzbach Mártonné: Az informatikai rendszerek életciklusa, Doktoranduszi Konferencia, 2001. novemberi konferencián elhangzott elõadások anyaga, 295 p.

- Schutzbach Mártonné: Matematikai modellek és módszerek a védelmi informatikában, az adattitkosítás kockázatelemzése, "Tavaszi Szél" 2000, 2001, a konferencia utókiadványa (posztergaléria), 125 p.

Mellékletek