ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM

Schutzbach Mártonné

Az informatikai rendszerek biztonságának kockázatelemzése a védelmi szférában

című doktori (PhD) értekezésének
szerzői ismertetése

Témavezető:

Dr. Kun István **a Gábor Dénes Főiskola főiskolai tanára**

Budapest, 2004

1. A tudományos probléma megfogalmazása

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 megkezdődött az informatikai biztonsági értékelés követelményrendszerének kidolgozása. A későbbiekben, 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.

Az informatikai rendszerek biztonságának megteremtése a gyors fejlődés, a fenyegető tényezők változása és a megfelelő biztonsági intézkedések bevezetése miatt nehéz feladat és mindig új problémákat vet fel.

A 2001. szeptember 11-én történt Amerika elleni terrortámadás arra is rámutatott, hogy az informatikai vezetőknek és a rendszeradminisztrátoroknak fel kell készülniük a legváratlanabb eseményekre is.

Az informatikai rendszerek egyre nagyobb mértékű alkalmazása az előnyök mellett új veszélyekkel és kockázatokkal jár a NATO szövetségi, a nemzeti és a védelmi szféra infrastruktúrára nézve is. A védelem megvalósítására, a biztonság megőrzésére a NATO rendszerekben többszintű védelmet kell alkalmazni a védendő rendszerek fontosságának megfelelően, és el kell fogadni azt a helyzetet, hogy nincs tökéletes biztonság.

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. Hazánk 2004-ben az Európai Unió tagja lesz. A biztonsággal foglalkozó szakembereknek vizsgálni kell, hogy az euroatlanti csatlakozásnak milyen hatása van a biztonsági követelményekre.

Az előzőek figyelembevételével az alábbi következtetéseket vontam le:

- Az informatikai biztonság problémaköre előtérbe került, elvi és gyakorlati kérdései is a kutatások napirendjén van.
- Nemzetközi és hazai szinten is igény van az egyeztetett követelmények kialakítására.

- Az informatikai biztonság megteremtéséhez fel kell tárni a fenyegető tényezőket, hogy védekezni lehessen ellenük. A fenyegető tényezők sokszínűsége miatt a feltárást részletesen több oldalról megközelítve kell elvégezni.
- A tökéletes biztonság elérése illúziónak tűnik, így előtérbe kerül a kockázatelemzés, amelynek során meghatározandók a védendő adatok fontossága, értéke. A veszélyek figyelembevételével lehet dönteni a meghozandó intézkedésekről, a védelmi szintről, amely arányos a védendő értékkel. Eldöntendő, hogy az így visszamaradt kockázat elviselhető-e, a *nem elviselhető maradvány-kockázat* újabb biztonsági intézkedések meghozatalát teszi szükségessé.

2. Kutatási célok

A téma választásakor értekezésem céljául tűztem ki a következőket:

- Olyan **kockázatelemzési módszereket, módszertanokat tanulmányozok, hasonlítok össze**, amelyeket már sikeresen alkalmaztak az informatikai rendszerek biztonságának elemzésénél, abból a meggondolásból, hogy az erősségek és a gyengeségek vizsgálatából hasznosítható következtetéseket vonhassak le a fő cél, a védelmi szféra informatikai rendszereinek vizsgálatára alkalmazható módszer, megvalósításához.
- **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.
- Továbbá célom **az informatikai biztonságot fenyegető tényezők teljesebb, több részletre kiterjedő feltárása és rendszerezése**, mivel a kockázatelemzés sikeressége nagy mértékben függ a fenyegető tényezők ismeretétől.

3. Kutatási módszerek

A kitűzött célok elérése érdekében a kutató munkám során az alábbi módszereket alkalmaztam:

- Tanulmányoztam a dolgozat témájával kapcsolatos hazai és nemzetközi szakirodalmat, a biztonságra vonatkozó főbb nemzetközi szabályozókat, a hatályos jogszabályokat.

- Konzultációt folytattam a Zrínyi Miklós Nemzetvédelmi Egyetem, a Gábor Dénes Főiskola, a Bolyai János Katonai Műszaki Főiskola, a Budapesti Műszaki és Gazdaságtudományi Egyetem, a Kürt Computer Rendszerház Rt., a Synergon Informatikai Rt., Takarékbank Rt., a Somogy Megyei Katasztrófavédelmi Igazgatóság, a Fővárosi Polgári Védelmi Igazgatóság biztonsági szakemberivel az informatikai biztonsággal kapcsolatos kérdésekről.
- Konferenciákon vettem részt, egy részről azért, hogy az informatikai biztonságról kialakított elképzeléseim minél nagyobb nyilvánosságot kapjanak és a véleményeket, megállapításokat a további munkámban figyelembe vegyem, másrészről a konferenciák megállapításait, irányzatait hasznosíthassam.
- Vizsgáltam a szakirodalomban előforduló, leggyakoribb kockázatelemzési módszereket, törvényszerűségeket tártam fel, levonható következtetéseket és hasznosítási lehetőségeket soroltam fel.
- Elemeztem a kockázatkezelésnél alkalmazott matematikai módszerek lehetőségeit.
- A védelmi szféra egy területének informatikai rendszerét vizsgáltam, és a kidolgozott kockázatelemzési módszer néhány lépését alkalmaztam.
- Értékeltem kutatásaim, tapasztalataim és megfigyeléseim eredményeit.

4. Az elvégzett vizsgálatok leírása (az értekezés felépítése)

Az értekezésben a választott témát az alábbi fejezetekben dolgoztam fel:

- A **bevezetésben** a téma kidolgozásának motivációit soroltam fel, megfogalmaztam a célokat, az alkalmazott módszereket.
- Az **első fejezetben** az informatikai biztonság megteremtésének lehetőségével foglalkoztam, áttekintettem a biztonságra vonatkozó főbb nemzetközi szabályozókat, hatályos jogszabályokat, biztonsági szabványokat. Kiemeltem a védelmi szféra informatikai biztonságának sajátosságait. Vizsgáltam az informatikai rendszerek életciklusának hatását a biztonságra.
- A **második fejezetben** a kockázatelemzési módszerek vizsgálatával, összehasonlításával, elemzésével arra a kérdésre kerestem a választ, hogy a nagyszámú kockázatelemzési módszert hogyan lehet alkalmassá tenni, kiegészíteni, vagy ilyen eljárást kialakítani a védelmi szféra informatikai rendszereire történő alkalmazáshoz. Az összehasonlításban a CRAMM, az ITB 8. számú ajánlása, a

COBIT, a MARION és az IT-Grundschutzhandbuch szerepel. A kiválasztásnál a következő szempontokat vettem figyelembe:

- Az informatikai biztonság témakörét hazánk uniós csatlakozása miatt célszerű az Európai Unió tagországaiban vizsgálni.
- Az összes létező 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.

Felsoroltam a kiválasztott módszerek pozitívumait, negatívumait és összehasonlítottam őket a következő szempontok szerint:

- Színvonal
- Függetlenség
- Minősíthetőség
- Realizálhatóság
- Alkalmazhatóság
- Értékelési terjedelem
- Eredmény-ábrázolás
- Gazdaságosság
- Aktualizálás
- Felhasználóbarát tulajdonság

A vizsgált módszerek összehasonlító szempontok szerinti értékelését grafikus megjelenítéssel tettem szemléletesebbé.

Ebben a fejezetben a leggyakoribb veszélyelemző módszereket, a hibafa elemzést, az eseményfa elemzést, a hibamód és -hatás elemzést, a veszély- és működőképesség elemzést, a hibamód, -hatás és kritikusság elemzést is vizsgáltam, valamint szükségesnek láttam egy sajátos matematikai módszer, a fuzzy elmélet felhasználhatóságát is bemutatni a kockázatkezelésben. 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 kockázatelemzésnél használt *nem jól definiált fogalmaknál* (pl.: kicsi, közepes, nagy) a megfelelő halmaz határait nem tudjuk egzakt módon meghatározni. Ebben az

esetben az elemek halmazhoz tartozása nem minden esetben dönthető el egyértelműen, így annak mértékét egy folytonos skála megfelelő értékével jelöltem. A fuzzy logikával támogatott kockázatelemzés előnyeit a következő pontokban foglaltam össze:

- Lehetőség van a számszerű eredmények további felhasználására.
- A rendszer egyszerű felépítésű, a szabálybázis felépítése könnyen érthető.
- Precíz és pontatlanul definiált adatokat egyaránt tud kezelni.
- Szemléletmódja közel áll az ember napi valóság-szemléletéhez.

- A **harmadik fejezet** módszertani útmutatót ad a védelmi szféra informatikai rendszereinek kockázatelemzéséhez. Kiemeltem azokat a legfontosabb okokat, amelyek megerősítették az elhatározásomat, hogy egy új módszertant dolgozzak ki a védelmi szféra informatikai rendszereinek vizsgálatára..

  A fejezet tartalmazza a kockázatelemzés egyes lépéseinél használható eszközöket, amelyek a kapcsolattartást, az áttekinthetőséget, az informatikai rendszer, a szervezet megismerését, a fenyegető tényezők feltárását segítik.

  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 legcélravezetőbbnek:

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

  Az öt lépéses módszertan előnyeit a jó áttekinthetőségben, a gyakorlati megvalósíthatóságban látom. Lényegesnek tartottam a kockázatelemzés egyes lépéseinek a gyakorlatban való megvalósíthatóságának bemutatását is. A kiválasztott szegmens a védelmi szféra egy részterülete, a Fővárosi Polgári Védelmi Igazgatóság informatikai rendszere.

  A fenyegető tényezők sokfélesége miatt rendszerezést, csoportosításokat készítettem, ennek során fokozottan figyelembe vettem a védelmi szféra informatikai rendszereit veszélyeztető tényezőket.

- Egy informatikai rendszer teljes körű kockázatelemzése nagy feladat, az áttekinthetőség miatt célszerű valamilyen felosztást végezni. A **negyedik fejezetben** az egyes részterületek közül a környezeti infrastruktúra, az alkalmazások, a rejtjelezés és a hálózatok sajátos kérdéseivel foglalkoztam.

  A környezeti infrastruktúra elemzése magában foglalja a számítóközpont épületének területét, magát az épületet, az épületben lévő 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 célszerűnek tarthatja.

  Az informatikai alkalmazások megfelelő szintű működése fontos területe az informatikai biztonságnak, ezért nagyobb részletességgel foglalkoztam az igényelt rendelkezésre állással, a becsült anyagi kárral, a meghibásodási valószínűségekkel, amelyek alapján a megfelelő pontértékekből a kockázat meghatározható.

  A rejtjelezés alapvető feladata algoritmikus eszközökkel biztosítani azt, hogy védett adatok csak az azok felhasználására kijelölt körben legyenek érthetők. Kiemeltem az alapvetően használatos kétféle rejtjelezési módszer, a szimmetrikus és az aszimmetrikus kulcsú, előnyeit és hátrányait. Foglalkoztam a nyilvános kulcsú rejtjelezés algoritmusai alapjául szolgáló matematikai problémákkal és felhasználásukkal. Megvizsgáltam a számítástechnikai rendszerek fejlődésének hatását a rejtjelezés biztonságára. Figyelembe vettem, hogy a gyakorlatban az adatok illetéktelenek kezébe jutásának általában rejtjelezés feltörhetőségén túl, sokkal inkább a kommunikációs csatorna nem megfelelő védelme vagy emberi tényezők, az adatkezelés nem megfelelően biztonságos szervezése az oka.

  Az egyre nagyobb hálózatok számos előnye mellett, a biztonságot érintő kockázati tényezők nagy mértékben növekedtek. Ez nem azt jelenti, hogy a jövő az egyedi gépeké, de a megfelelő biztonsági intézkedések nélkül létrehozott hálózati csatlakozás nem lebecsülendő veszélyeket rejthet. Ebben az alfejezetben rendszer-összeomlásokkal, csalásokkal, nagyobb hibákkal, támadások vizsgálatával, számítógépes vírusokkal, férgekkel, trójai programokkal foglalkoztam. Egy szervezet hálózatának biztonsága érdekében a gyakorlatban már bevált lépéseket lehet tenni, mint például biztonsági intézkedések meghozatala, biztonsági terv kialakítása, tűzfalak telepítése, betörésvédelmi rendszerek alkalmazása vagy a legfrissebb vírusirtó szoftverek használata. Az elemzés során a gyakorlatban már jól bevált lépések megvalósítását kell vizsgálni. A külső támadások vizsgálatánál, a kockázatelemzés

egyik segítője lehet az „ethical hacking” (etikus hackelés) eljárás. A hackelésből származó ismereteket jól képzett szakemberek vagy szakemberek csoportja a vizsgált szervezet érdekében tudja hasznosítani.

Mivel a kockázatelemzési eljárás sikere nagy mértékben függ a fenyegető tényezők minél teljesebb körű feltárásától, annak érdekében, hogy ez a számbavétel ne legyen hiányos, a fenyegető tényezőket első megközelítésben *humán, logikai, fizikai és környezeti tényezők csoportjába rendszereztem*.

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

Az előbbi rendszerezéseken túl, elősegítheti a veszélyelemzést a *veszélyeztető faktorok katalógusána*k felépítése. Ebből kiindulva is bemutattam a fenyegető tényezők rendszerét, öt szempont szerinti osztályozásban, ez a csoportosítás a felelősség kérdését is sugallja.

- Az **utolsó fejezet** tartalmazza az eredmények összegzését, következtetések levonását, az értekezés felhasználhatóságának elemzését, a további kutatási irányok felvetését.

5. Összegzett következtetések

Az értekezés kutatási céljaként megjelölt kérdések részletes kifejtését és elemzését az egyes fejezetekben külön-külön elvégeztem. Az egyes kutatási célok elérésével kapcsolatosan az alábbi összegzett következtetéseket vontam le:

- **Meghatároztam** azokat az alapfogalmakat, amelyeket az értekezésemben használtam, **áttekintettem** az informatikai biztonság kialakítása során figyelembe veendő jogszabályokat, szabványokat és ajánlásokat, **rendszereztem** a biztonsági osztályokra vonatkozó egységes követelményeket.
- A védelmi szféra érdekeinek figyelembevételével **kiválasztottam** különböző kockázatelemző 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 veszélyelemző módszer (a hibafa és eseményfa) megvalósíthatóságát. **Összegeztem** az informatikai rendszerek teljes életciklusán végigvezető veszélyelemzési folyamatokat.
- **Kidolgoztam** egy kockázatelemzési módszertani útmutatót a védelmi szféra informatikai rendszereinek kockázatelemzésére. **Kialakítottam** az informatikai biztonságot fenyegető tényezők rendszerét.
- **Kiemeltem** az informatikai rendszer egyes részterületeit, **ráirányítottam a figyelmet** az adott részterület biztonsági vizsgálatának releváns tényezőire.

6. Új tudományos eredmények

Az informatikai rendszerek biztonságának kutatása során elért tudományos értékű 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 fenyegető tényezők rendszerének kialakítását.**

7. A kutatási eredmények felhasználhatósága, ajánlások

A téma kidolgozásával hozzá kívántam járulni;

- az informatikai biztonság kérdéskörének elméleti és gyakorlati továbbfejlesztéséhez,
- a felsőfokú oktatásban használható informatikai védelmi infrastruktúrák továbbfejlesztéséhez,
- az informatikai rendszereket fenyegető támadások felismeréséhez, mivel ez a felismerés az első 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 fenyegető tényezők figyelemmel kísérésénél, ami segíti a veszélyhelyzetek megelőzését.
- Az általános módszertan a védelmi szféra informatikai rendszereinek kockázatkezelésénél közvetlenül vagy a változások figyelemmel kísérésével kisebb módosításokkal alkalmazható.
- Az eredményeim nemcsak a védelmi szféra működési területén hasznosíthatók, hanem pl. banki, kormányzati területeken is támogatják a felhasználót.
- A felsőfokú oktatásban, a kutatómunkában közvetlenül hasznosíthatók az összehasonlító elemzések.
- A kidolgozott veszélyelemzési módszerek alkalmazhatók megelőzési célból, a védelmi szféra informatikai rendszereit fenyegető veszélyek vizsgálatában.