HADMÉRNÖK

XII. Évfolyam 3. szám – 2017. szeptember

# KOCKÁZATKEZELÉS, TUDOMÁNY VAGY KURUZSLÁS?

## RISK MANAGEMENT, SCIENCE OR SWINDLE?

MEGYERI Lajos; FARKAS Tibor
(ORCID ID); (ORCID ID: 0000-0002-8868-9628)
megyeri.lajos@uni-nke.hu; farkas.tibor@uni-nke.hu

***Absztrakt***

*A cím meghökkentő lehet. De a kockázatok felmérése egyfajta jövőbelátási törekvés, amelyben előre szeretnénk tudni, mi fog történni, hogy előre védekezhessünk ellene, mégpedig a legjobb módszerrel, a megelőzéssel. Véleményünk szerint a kockázatkezelési eljárásoknak nagy változásokon kellett keresztülmenniük, amíg a misztikumból a tudományig jutottak, és ez az út még nem ért véget.*
*Jelen cikkben a teljesség igénye nélkül a kockázatelemzés különböző megközelítési módjain át el kívánunk jutni az informatikai rendszerek kockázatkezelésének jogi szabályozásáig és végrehajtásának lehetőségeihez, nem térünk ki részletesen a kockázatkezelés matematikai modelljeinek leírására.*
*„Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült”*

**Kulcsszavak:** *biztonság, jogszabály, kockázat, menedzsment, sebezhetőség, fenyegetés*

***Abstract***

*The title may be strange. But risk assessment is a sort of forward looking ambition in which we want to know what is going to happen to defend ourselves against it, by the best method of prevention. In our opinion, risk management procedures had to go through great changes as long as mystics came to science, and that path did not end there.*
*Without the need for completeness in this article we would like to go through the different approaches to risk analysis to the legal regulation of risk management of IT systems and the possibilities for implementing them, we will not describe in detail the mathematical models of risk management.*
*“This article was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.”*

**Keywords:** *security, laws, risk, management, vulnerability, threat*

A kézirat benyújtásának dátuma (Date of the submission): 2017.07.01.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.09.25.

## BEVEZETÉS

Napjainkban végbemenő események egyre erőteljesebben támasztják alá, hogy a védelmi szektor minden területének folyamatos megújulása és fejlesztése nélkülözhetetlen, amelynek egyik vezérfonala a biztonság, valamint annak az információ védelmére irányuló tevékenysége. Mindezek alapján nagy hangsúlyt kell fektetni napjaink kutatásai során ezen területre, amelyet a Nemzeti közszolgálati Egyetem tudományos kollégiumai is megfogalmaztak összefoglaló közleményükben. [1], [2] Ennek alapján jelen közlemény a kockázatkezelést vizsgálja különböző megvilágításban.

A kockázatkezelés egyidős az emberiséggel. A gondolkodó ember mindig igyekezett az életét a lehető legtovább megőrizni. Az emberi közösségek már kialakulásuk kezdetén úgy szerveződtek, hogy tagjaik biztonságban érezzék magukat, hiedelmekkel, vallással, tudománnyal, a társadalmi lét minden területét úgy alakították, hogy a bolygón való létezést össztársadalmi szinten működő és kiszámítható rendszerekben éljék. Az ősközösség és az ókori társadalmak kialakulásakor fenyegetést elsősorban a természeti csapások jelentették, az ellenük való védekezés megfelelő szintje nyújtotta a biztonságot. Hamarosan az ember lett a legfőbb fenyegetés embertársára, ettől kezdve erős államok és hadseregek próbálták biztosítani a biztonságot saját polgáraiknak a többiekkel szemben. Ez napjainkig húzódó folyamat, jelenleg a NATO legfőbb célkitűzése a tagországok biztonságának szavatolása.

A kockázatok becslésére már az emberi gondolkodás kezdetétől két egymástól gyökeresen különböző eljárás alakult ki, melyeket olykor egymás kiegészítésével használtak. Nagy események, mint csaták, házasság kötések, szövetségre lépés előtt a döntéshozó vezetők biztosak szerettek volna lenni abban, hogy jó úton járnak, igyekeztek minél kisebb kockázatú döntéseket hozni.

Egyik lehetőség volt a mágus, varázsló, táltos, aki csontokból, tűzből és egyéb áldozati ereklyékből „megjósolta” a jövőt. Ennek „tudatában” hozta meg a vezető a döntést. A másik irány a tudomány.

Szembenálló erők számvetése, létszám, fegyverzet, terepviszonyok elemzése. Szun Ce „A hadviselés törvényei” című, időszámításunk előtti ötödik században írott munkájában már sok különböző számvetést sorol fel, amelyeket a vezérnek figyelembe kell vennie, ha győzni akar. Egyfajta sebezhetőségi listaként is felfogható az ellenség lehetséges gyenge pontjainak az ismertetése. A történelem során minden sikeres hadvezérnek kellett ilyen számvetéseket, értékeléseket végeznie, ha nem is nevezték a tevékenységet kockázatelemzésnek.

A hadtudományok azóta is folyamatosan fejlesztik a küzdelem megvívásának optimális eljárásait. Mindezek mellett a mai napig papi áldás kíséri a csapatzászlókat és a hadba induló katonákat, mert minden kockázatot a tudomány nem tud ellensúlyozni – kezelni.

A mai modern világban, a tudományágak specializálódása révén a kockázatkezelésnek is komoly ismeretanyaga gyűlt össze az élet legkülönbözőbb területein. Legnagyobb múltra és tapasztalatra véleményem szerint a biztosító társaságok kockázatelemzései tekintenek vissza. Ott egyértelműen, szerződésben rögzítve vannak a vagyontárgyak, kockázati értékek. Az életbiztosítások esetén még az emberi élet és testi épség elvesztése is kifejezhető pénzben.

Teljes biztonság állapotáról természetesen sohasem beszélhetünk. Minden élőlény, tárgy, rendszer, társadalom sebezhető. A biztonság megteremtésére sehol nem áll rendelkezésre végtelen idő, pénz, munkaerő. Szükség van az erőforrások ésszerű felhasználására, ebben nyújt segítséget a kockázatok feltérképezése, elemzése.

A számítástechnikai eszközök rohamos fejlődése nagy kiterjedésű informatikai hálózatok kialakulásához vezetett, (pl. Internet). Az informatikai hálózatok kezdetben ad hoc jelleggel, egymástól függetlenül fejlődtek. Egy bizonyos szintet elérve, az interoperabilitás érdekében az informatikai hálózatok tervezői kénytelenek voltak közös eljárásrendeket kialakítani. A rendszerek méretének és bonyolultságának a növekedésével egyre nőtt a rendszerelemek sebezhetősége is. Szabványrendszerek alakultak ki, melyek mindegyikében megjelent az

informatikai kockázatkezelés szükségessége. Jelen közleményben a kockázatkezelés általános eljárásrendjein túl az informatikai rendszerek kockázatkezelésével kapcsolatos szabályozókat és a kockázatkezelés végrehajtásának lehetőségeit foglaljuk össze.

## KOCKÁZATKEZELÉS ÁLTALÁBAN

A várható hatás tekintetében a kockázatok két nagy csoportra oszthatók. Az első csoportba az úgynevezett egyszerű (tiszta, pure) kockázatok tartoznak, melyek esetében a lehetséges kimenetelek az alábbiak lehetnek: (a) kár, veszteség következik be,(b) vagy nem következik be semmilyen változás. Ezzel szemben összetett (speculative) kockázatról akkor beszélünk, ha a vizsgált kockázathoz háromféle kimenetel tartozhat: (a) kár, veszteség következik be; (b) nem történik változás;(c) nyereség, gyarapodás az eredmény. [3]

A mezőgazdaságban például összetett kockázatvállalásról beszélhetünk, amikor a gazda eldönti, hogy mit vet a földbe. Különböző terményeknek más-más a megtérülési rátája – haszna, de eltérő mértékű a vállalt kockázat is. A gazda átgondolhatja, mekkora kockázatot vállal milyen haszon reményében.

Az informatikai rendszerek esetében a kockázatvállalás önmagában nem eredményez kimutatható nyereséget. Ha védelmi rendszerünket a kockázat elemzésnek köszönhetően jól alakítjuk ki, akkor nem következik be kár, veszteség. Ezért nehéz a tulajdonost, döntéshozót rábírni arra, hogy anyagi erőforrásokat fordítson a biztonságra, mert az ebből fakadó „elmaradt kár” nehezen mutatható ki mindaddig, amíg valós biztonsági esemény kapcsán veszteség nem éri a tulajdonost.

### Banki szféra, biztosítók

#### *A biztosítási szolgáltatások*

A mai modern biztosítási szolgáltatások eredete a céhes időkre vezethetők vissza. Az 1300.-as évektől képeztek pénztartalékot a céhtagok „megszorulása” esetére. A napóleoni háborúk alatt a hadsereg logisztikai ellátmányának biztosítására alakult az első formális biztosító, melyet azóta számos hazai és nemzetközi társaság követett

A banki szolgáltatások egyik legrégebbi és alapvető, egyben legrizikósabb típusa a hitelezés. Hitel nyújtásának téves megítélése esetén, - különösen, ha több alkalommal, vagy nagy összegre szóló ügyletre terjed ki - a bank könnyen csődbe mehet. Ezért a hitelezési kockázat vállalását hazai [4] és nemzetközi jogszabályok szigorúan keretbe foglalják. A szabályok pontosan rögzítik a kockázatvállalás elveit, kidolgozandó dokumentumait. A pénzintézeteknek kockázatvállalási szabályzatot kell készíteniük, minősíteniük kell az adósokat (mint potenciális fenyegetéseket) amely minősítést egy informatikai rendszerben tárolnak és bármely pénzintézet számára hozzáférhetővé teszik. A modern biztosítás ismeretek szerint a kockázat:

*„A biztosítási ügyek szempontjából az eredményeknek a kitűzött célokhoz viszonyított kedvezőtlen (negatív) eltéréséből fakadó anyagi veszteségeket tekintjük kockázatnak. A veszteségnek pénzben kifejezett ellenértéke a kár. A kockázatok kezelésének tudományos, összehangolt, egységes és gazdasági optimumot kereső módszerét nevezi a szakirodalom risk managementnek, a legjobb magyar megfelelője talán a kockázatkezelés. A kockázatokkal tudatosan szembenéző egyén, intézmény által alkalmazott koordináló, integráló és optimalizáló elméleti és gyakorlati módszertan a kockázatkezelés.”*. [5]”

Tehát a biztosító társaságok egyértelműen a gazdasági megfontolások alapján kezelik a kockázatokat. A kockázatok kiszámíthatósága érdekében úgynevezett veszélyközösségeket alakítanak ki. A nagy számok törvénye alapján a veszélyközösség egészére könnyebben kalkulálható a biztosítás díja. Ezzel a megközelítéssel matematikai képletek, illetve egyre inkább a célnak megfelelően fejlesztett szoftverek segítségével kalkulálhatják ki a kockázat

árát, amit minden esetben az ügyféllel fizettetnek meg. Előfordulhatnak nagy kockázatú, esetleg előre láthatóan veszteséges biztosítási ágazatok. Ebben az esetben, ha a biztosítási rendszer fenntartása közösségi érdek, az állam beavatkozhat, és kötelezhet biztosítókat arra, hogy a nyereséges üzletágak mellett a veszteségeset is fenntartsa, ehhez állami hozzájárulás is adhat. Itt kiemelkedő fontosságú a tapasztalatok alapján elkészített jövőre vonatkozó üzleti terv, melynek alapvető eleme lehet a kockázatelemzés.

### *Közgazdasági szféra*

Az üzleti vállalkozások tevékenysége pénzügyi kockázatokkal jár, a kockázatokat a tulajdonos és a befektetők tulajdonosai tudatosan, a haszon reményében vállalják. A vállalati befektetés számos más befektetési formánál súlyosabb kockázattal jár, ezért itt a befektetők nagyobb nyereséget, gyorsabb megtérülést várnak el. Ezt az igényt gyakran a kockázatmentes, vagy alapkockázatúnak tekintett államkötvény-hozamhoz viszonyított többletként határozzák meg, százalékpontban kifejezve. [6]

Modellek:

COSO ERM keretrendszer A COSO (Committee of Sponsoring Organizations of Treadway Commission) szervezésében a 90-es évek elején összeállított és folyamatosan fejlesztett vállalati kockázatkezelő (EnterpriseRisk Management) keretrendszer a vállalat belső folyamataira, azok szabályozására és ellenőrzésére vonatkozik. [7] A rendszer lényege, hogy vállalati szintű egységes kockázatkezelési rendszert kell létrehozni, a kockázatokat súlyozzák, a részterületeknek személyes felelősei vannak, a kockázatokat folyamatosan mérik – elemzik.

Az ISO 31000:2009 [8] egy nemzetközi szabvány, amely irányelveket határoz meg a kockázatfelmé-réssel és kezeléssel kapcsolatosan. Ezt a szabványt bármilyen tulajdonformába tartozó (magán, állami) vállalkozások, szervezetek alkalmazhatják. Az ISO 31000:2009 szabvány a szervezetek működése során, a szervezeti tevékenységek, folyamatok széles körére alkalmazható, beleértve a stratégiaalkotást és döntéshozatali mechanizmust, működést, folyamatokat, funkciókat, projekteket, termékeket, szolgáltatásokat és eszközöket. A nemzetközi szabvány a negatív kimenetelű, bármilyen típusú kockázat mellett, a pozitív kimenetelű kockázatok esetében is alkalmazható. Az ISO 31000:2009 szabvány alapján a kockázatot, a bizonytalanság vállalati célokra való hatásaként értelmezik, így a kockázatkezelés folyamata a vállalati célrendszer egymásra épülő szintjein keresztül mutatható be. A kockázatfelmérésre és kezelésre vonatkozó tervek és keretrendszer megtervezése és végrehajtása során figyelembe kell venni a szervezetek speciális céljait, környezetét, struktúráját, folyamatait, projektjeit, termékeit, szolgáltatásait, eszközeit, és a szervezetek által alkalmazott speciális gyakorlatokat Az ISO 31000:2009 Risk Management szabványa többi ISO szabványtól eltérően nem tanúsítható, de megfelelő keretet nyújt a vállalatok által alkalmazott és/vagy fejlesztendő kockázatkezelési gyakorlatok áttekintésére. A szabvány által meghatározott alapelvek segítenek a kockázatkezelés vállalatirányítási keretekbe történő illesztésének megvalósításában. [9]

*Gordon-Loeb Model:*

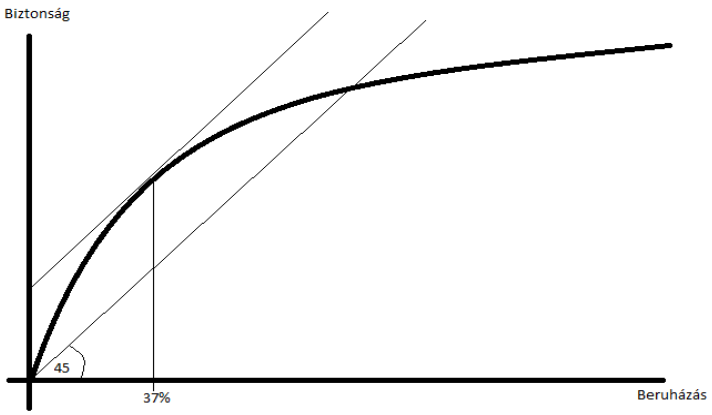
2002-ben Gordon és Loeb [10] egy egyszerű és nagyon általános modellt javasolt a sebezhetőség csökkenésének értékelésére. A Gordon-Loeb / gȯr-dən lōb / modell egy matematikai gazdasági modell, amely elemzi az optimális befektetési szintet az információbiztonságban.

A modellből arra lehet következtetni, hogy az információ védelmére törekvő vállalkozásnak általában véve a várható veszteségnek csak egy kis része következik be (a cyber információbiztonság megsértéséből eredő veszteség várható értéke). Pontosabban, a modell azt mutatja, hogy általában nem gazdaságos az információbiztonsági tevékenységekbe (ideértve a számítógépes biztonságot vagy a számítógépes biztonsággal kapcsolatos tevékenységeket) fektetni nagyobb összeget, mint a biztonság megsértéséből származó

várható veszteség több mint 37 százalékát (lásd 1. számú ábra). A Gordon-Loeb modell azt is mutatja, hogy egy adott szintű potenciális veszteség esetén az információs készlet védelmére fordított optimális összeg nem mindig növekszik az információs rendszer sebezhetőségének növekedésével. Más szóval, a szervezetek nagyobb megtérülést tudnak nyújtani biztonsági tevékenységeikben a cyber / információbiztonsági tevékenységekbe történő befektetéssel, amennyiben erőfeszítéseik a közepes szintű sebezhetőségek biztonságának javítására irányulnak.

A Gordon-Loeb modellt először Lawrence A. Gordon és Martin P. Loeb publikálták 2002-ben, az ACM Információs és Rendszerbiztonsági Transzakonciák című, "Az információbiztonsági befektetések gazdaságossága" címû kiadványában.

A modell tehát azt mutatja, hogy egy információs rendszer kiberbiztonsági tevékenységeire fordítandó összeg növelése egy bizonyos határon túl nem gazdaságos az információs rendszer sebezhetőségének kezelésére.




**1. ábra** A Gordon-Loeb modell [11]

A modell szerint először fel kell mérni a védendő vagyontárgyak értékét alacsonytól magas szintig. Ezután meg kell vizsgálni a rendszer elemeinek sebezhetőségét alacsonytól magas szintig. Ezután összevetve az értékek és sebezhetőségek táblázatát, meg kell határozni azokat az elemeket, melyek sebezhetőségét csökkenteni fogjuk. A modell szerint a magas értékű, de közepes sebezhetőségű elemek védelme nyújt gazdaságos egyben kielégítő védelmet. [12]

### *Költségvetési szervek kockázatkezelése*

A költségvetési szervek gazdasági tevékenységével kapcsolatban a „Folyamatba épített előzetes, utólagos és vezetői ellenőrzés” rendszerét (a továbbiakban FEUVE) 2011. évi CXCV. törvény és végrehajtásáról szóló 368/2011. (XII. 31.) kormányrendelet, illetve a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről szóló 370/2011. (XII. 31.) Korm. rendelet határozza meg. Ez utóbbi szerint:” *integrált kockázatkezelési rendszer: olyan folyamatalapú kockázatkezelési rendszer, amely a szervezet minden tevékenységére kiterjed, egységes módszertan és eljárások alkalmazásával, a szervezet célkitűzéseinek és értékeinek figyelembevételével biztosítja a szervezet kockázatainak teljes körű azonosítását, azok meghatározott kritériumok szerinti értékelését, valamint a kockázatok kezelésére vonatkozó intézkedési terv elkészítését és az abban foglaltak nyomon követését. Kockázatelemzés: objektív módszer az ellenőrizendő területek kiválasztására, mely meghatározza a költségvetési szerv tevékenységében és belső kontrollrendszerében rejlő kockázatokat*” [13]

A lényeg tehát, hogy a szervezet minden tevékenységi körében értelmezi és értékeli a kockázatokat. A tevékenységek szabályos működését név szerinti, személyes felelősséghez köti. Az elemzést (FEUVE) minden naptári évben el kell végezni, a személyi felelősökkel meg kell ismertetni és a szervezet vezetőjének jóvá kell hagynia.

A FEUVE rendszere a következő bontásban határozza meg a kockázatelemzés elkészítését:

*Külső kockázatok*

Infrastrukturális: Az infrastruktúra elégtelensége vagy hibája megakadályozhatja a normális működést.

Gazdasági: Az infláció negatív hatással lehet a tervekre. Jogi és szabályozási A jogszabályok és egyéb szabályok korlátozhatják a kívánt tevékenységek terjedelmét. A szabályozások nem megfelelő megkötéseket tartalmazhatnak.

Politikai: Egy kormányváltás megváltoztathatja a kitűzött célokat, a célok prioritását. Piaci Szállítói probléma negatív hatással lehet a tervekre.

Elemi csapások: Tűz, árvíz vagy egyéb elemi csapások hatással lehetnek a kívánt tevékenység elvégzésének képességére. A katasztrófavédelmi terv elégtelennek bizonyulhat.

*Pénzügyi kockázatok*

Költségvetési: A kívánt tevékenység ellátására nem elég a rendelkezésre álló forrás. A források elosztása nem befolyásolható közvetlenül

Pénzügyi Eszközvesztés. A források nem elegendőek a kívánt megelőző intézkedésre.

*Tevékenységi kockázatok*

Működés-stratégiai: Nem megfelelő stratégia követése. A stratégia elégtelen vagy pontatlan információra épül. Működési Elérhetetlen/megoldhatatlan célkitűzések. A célok csak részben való- sulnak meg.

Információs: A döntéshozatalhoz nem megfelelő információ a szükségesnél kevesebb ismeretre alapozott döntést eredményez.

Hírnév: A nyilvánosságban esetlegesen kialakult rossz hírnév negatív hatást fejthet ki.

Technológiai: A hatékonyság megtartása érdekében a technológia fejlesztésének/lecserélésének igénye. A technológiai üzemzavar megbéníthatja a működést.

Projekt: A megfelelő előzetes kockázatelemzés, hatástanulmány nélkül elkészülő projekttervezet. A projektek nem teljesülnek a költségvetési vagy funkcionális határidőre.

Újítás: Elmulasztott újítási lehetőségek. Új megközelítés alkalmazása a kockázatok megfelelő elemzése nélkül.

*Emberi erőforrás kockázatok*

Személyzeti: A hatékony működést korlátozza, vagy teljesen ellehetetleníti a szükséges számú, megfelelő képesítésű személyi állomány hiánya.

Egészség és biztonsági: Ha az alkalmazottak jó közérzetének igénye elkerüli a figyelmet, a munkatársak nem tudják teljesíteni feladataikat.

Mindezeken felül a költségvetési szervekre is érvényes a 2013 évi L törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, amely többek között kifejezetten az elektronikus információbiztonsággal kapcsolatos kockázatkezeléssel foglalkozik. A katonai információbiztonsági kockázatelemzés végrehajtásának lehetőségeivel, oktatásának buktatóival foglalkozik Kerti András.[14] Véleménye szerint az adat minősítése (korlátozott terjesztésű, bizalmas, titkos), már önmagában is egy kockázatelemzés eredménye. Ennek a részterületnek az elemzése túlmutat jelen cikkem terjedelmén, ezért részletesen a honvédelmi szervezetek kockázatkezelésénél kívánom kifejteni.

### *Veszélyes anyagokkal kapcsolatos baleseti veszély kockázatának elemzése*

A veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X. 20.) Korm. rendelet határozza meg,, hogy az üzemeltető csak a hatóság engedélye alapján folytathat veszélyes tevékenységet. A hatósági engedély kérelem benyújtásakor az üzemeltető

súlyos káresemény elhárítási tervet, biztonsági elemzést vagy biztonsági jelentést köteles készíteni.

A használt veszélyes anyagok típusától, mennyiségétől függően jellemezni kell a veszélyes tevékenységhez kapcsolódó infrastruktúrát és részletes elemzéssel be kell mutatni a veszélyes anyagokkal kapcsolatos legsúlyosabb baleseti lehetőségeket.

A következő ábra bemutatja a veszélyelemzés egy lehetséges eredményét:

| Létesítmény | Eseménysor | Feltételezett következmények | Értékelés |
|---|---|---|---|
| 1. sz. tartály | a) Katasztrofális törés | Üzem kerítését átlépő hatások | 5 |
| | b) 10'-en belüli teljes anyagvesztés | Üzemen belüli hatások, lehetséges belső dominóhatások | 4 |
| | c) Korróziós lyukadás 50 mm Ø | Üzemen belüli hatások | 3 |
| | d) Korróziós lyukadás 10 mm Ø | Más létesítményt is érintő helyi hatások | 2 |
| | e) Túltöltés | Helyi hatások | 1 |
| Átmeneti tároló (1 db 1 $m^3$-es acetonos IBC | a) Katasztrofális törés | Más létesítményt is érintő helyi hatások | 2 |
| | b) Tartály-lyukadás | Más létesítményt is érintő helyi hatások | 2 |
| | c) Tömítetlenség | Helyi hatások | 1 |
| | | | |

**1. táblázat** Veszély elemzés értékelése [15]

Nagy jelenősége van az elemzés elkészítésekor az elkészítendő szakvéleményeknek. Hazai példa a veszélyelemzés téves értékelésére:

A MAL Timföld kft Kolontári üzemének veszélyeztetés értékelése szerint: „A vörösiszap kazetták gátszakadása csak külső hatásra következhet be:

- nagy erősségű földrengés
- terrorcselekmény (rongálás, robbanás)
- háborús bombatámadás" [16]

Ezzel szemben a valóságban a kolontári vörösiszap kazetta az utólagos vizsgálatok szerint nem külső hatásra szakadt át. A baleset következtében 10 ember életét veszítette és felbecsülhetetlen kár keletkezett a természeti környezetben.

A veszélyes anyagokkal kapcsolatos veszélyelemzések elkészítésekor számos esetben szimulációs programot, szoftvert használnak.(például Relex 7.7, RiskCurves, RiskSpectrum Professional) [17]

Az elemzés eredménye nagyban függ attól, hogy a szimulációs program paraméterei mennyire közelítik meg a valóságot. A szoftverekben a legrosszabb esetre lehetséges paramétereket állítják be, a lehető legrosszabb következményekkel számolva. Ha a veszélyt jelentő következmények még így sem érik el az üzem külső határát, az üzemet a lakosság szempontjából biztonságosnak nevezik. Természetesen további rendszabályok és védő eszközök alkalmazása szükséges az üzemen belüli dolgozók védelme érdekében.

### *Létfontosságú rendszerek - Kritikus infrastruktúrák*

A „65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról” több helyen is megemlíti a létfontosságú rendszerek és létesítmények védelmével kapcsolatban a kockázatelemzés szükségességét. A kockázatelemzés fogalmát az alábbiak szerint határozza meg:

*„kockázatelemzés: fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából;”* [18]

A fogalom így szerintem nem letisztult, a kockázati tényezők vizsgálata alatt sok mindent lehet érteni. A jogszabály nem ad egyértelmű iránymutatást a kockázatelemzés végrehajtásának módszerére bár a kockázatok azonosításának és értékelésének a módját részletesen leírja:

A rendszerelemet fenyegető kockázati lista készítését határozza meg majd a kockázatok valószínűsíthető okainak feltárását írja elő a prognosztizálható negatív hatás meghatározásával együtt.

A kockázatok értékelését írja elő, majd a kockázatok kezelését a kockázati szint függvényében. Ez a metódusra véleményem szerint a CRAMM típusú kockázatelemzés képes bár a jogszabály a kockázatelemzés módját nem határozza meg.

A kockázatelemzés eredményét úgynevezett azonosítási jelentésben meg kell jeleníteni. Az üzemeltető a kockázati szinteknek megfelelően foganatosít biztonsági intézkedéseket a rendszerelem biztonsága érdekében.

A létfontosságú rendszerelemek Üzemeltetői biztonsági tervében szerepeltetni kell a főbb fenyegetettségek elemzését és az egyes elemek sebezhetőségén, valamint a lehetséges hatásokon alapuló kockázatelemzést. A jogszabály nem határozza meg, de véleményem szerint célszerű egy átfogó kockázatelemzés egyik részterületének tekinteni a rendszerelem információs infrastruktúrájának vizsgálatát és a részterület elemzését a szakmában járatos lehetőleg független szakemberekkel kell végeztetni.

Elmondható tehát, hogy a létfontosságú rendszerelemek tekintetében a kockázatelemzés megléte kötelező, tartalmi, módszertani megkötéseket azonban a jogszabály nem tartalmaz.
A jogszabály megemlíti a honvédelmi létfontosságú rendszerelem fogalmát is, értelmezésem szerint ezekre is vonatkoznak a fent leírtak, így elérkeztünk a honvédelmi célú infrastruktúrákhoz.

## KOCKÁZATKEZELÉSI MÓDSZEREK

### Kockázatkezelés alapvető formái

#### *Kockázatkerülés*

Bizonyos károk, veszteségek esélyének a teljes kiküszöbölését jelenti. Jelentheti azt, hogy a szervezet az elemzés alapjául szolgáló tevékenységével a kockázatok növekedése miatt felhagy. Általános, minden területre kiterjedő kockázatkerülés nem lehetséges, mert ez a vizsgált rendszer működésképtelenségét jelentené. Egyes szolgáltatások megszüntetése a túlzottan magas kockázat miatt azonban lehetséges.

#### *Kockázatok csökkentése*

Ez az elv jelenti az igazi kockázatkezelést, mert itt a kockázat csökkentésére a szervezet saját szervezési vagy hardver – szoftver eszközeit használjak fel. Az eljárások, melyek ebbe a csoportba tartoznak, három részre oszthatók.

A kármegelőző (pre-loss) elvek biztosítják azt, hogy a szervezet gazdaságosan, a jogszabályoknak megfelelően működjön. Itt nem az a cél, hogy teljes mértékű biztonságot

érjenek el, hiszen ez gyakorlatilag lehetetlen. Ebbe a csoportba tartozik az épületek, gépek, járművek, berendezések szabályszerű, rendszeres karbantartása, informatikai rendszerek védelmi rendszere, tűzfal, kártékony programok elleni védelem, szabályzatok, utasítások kidolgozása, betartása.
A másik csoport a kárenyhítést célozza. Az úgynevezett pro-loss vagyis kárenyhítő kockázatkezelés a károk bekövetkezésének megakadályozásával nem foglalkozik, mert itt a bekövetkezett károk hatásának enyhítése a cél. Alapvető követelmény a rendszer visszaállítása a lehető legrövidebb időn belül a lehető legkisebb adatveszteséggel. Fontos, hogy a szervezet alaprendeltetésből adódó működőképessége folyamatosan fennmaradjon.
A harmadik kategóriába tartoznak azok a vállalt kockázatok, melyek nem igényelnek semmiféle intézkedést. Ennél a stratégiai részterületnél a passzivitás az irányadó. Ezek olyan kockázatok melyek elhanyagolhatóak, elenyészőek, de mégsem illenek bele az előbbi két csoportba. Egyes terminológiákban ezt maradvány kockázatnak nevezik, melyet a szervezet vezetőjének írásban el kell fogadnia.

### *Kockázatmegosztás, kockázatáthárítás*

Ez esetben arról van szó, hogy a vállalat a kockázatok egy részét egyedül nem képes vagy nem kívánja vállalni, ezért áthárítja azokat. A partner lehet állami szervezet, hatóság, üzleti partner, befektetők, pénzintézetek, biztosítótársaságok. Az üzleti szerződések feltételeinek megfelelő alakítása lehet az egyik módja a kockázat áthárításának. A szerződés megkötésekor mérlegelni kell a kockázatokat és azok elosztását a szerződő felek között. A biztosítás is áthárító, kockázatmegosztó jellegű. Egy másik módszer a stratégiai szövetségek kötése. Ilyen lehet pl. a szoftverforgalmazók szövetségre lépése annak érdekében, hogy ezzel megakadályozzák a szoftverek illegális másolását, értékesítését. [19]

## Kockázat elemzés módszerei

### *Hibafa elemzés (FTA)*

Katasztrófavédelemhez kapcsolódó rendszerek, veszélyes üzemek biztonsági elemzéséhez használják. A módszer egyik alapvető előnye az, hogy olyan meghibásodási lehetőségek szisztematikus és logikus feltárására és feldolgozására alkalmas, amelyek súlyos baleset kialakulásához vezethetnek. Ez a fajta feldolgozás azt igényli, hogy az elemzést végző teljes mértékben ismerje és értse az üzem vagy a rendszer működését, valamint a berendezések különböző meghibásodásainak módjait.

A hibafa elemzés az eseményeket a súlyos balesethez vezető berendezés meghibásodásokra és az emberi tévedésekre bontja fel. A módszer ezért egy fordítva gondolkodási technika, azaz az elemző a súlyos balesetből, vagy a nemkívánatos esetekből indul ki. Ezeket el kell kerülni, és meg kell határozni az eseményt közvetlenül kiváltó okokat. Sorba vesszük a közvetlen kiváltó okokat, továbbá mindig megállapítjuk az eseményhez vezető alapvető okokat. A hibafa olyan ábra, amely szemlélteti ezeket az alapvető okokat, továbbá az okok és a baleset közötti összefüggéseket. Az ábrán „ÉS” „VAGY” kapuk jelölésével mutatják be, hogy bizonyos események együttes előfordulása eredményezhet negatív kimenetelt, ami további negatív eredményeket hozhat, ami végül a „csúcsesemény” mint lehető legrosszabb következmény megvalósulásáig vezet.

A hibafa elemzés eredménye azoknak a berendezés-hibák és az emberi hibák kombinációjának felsorolása, amelyek elegendőek egy súlyos baleset kiváltásához. A meghibásodásoknak ezeket a kombinációit minimális hibaesemény kombinációnak nevezik. Mindegyik minimális hibaesemény kombináció a berendezés- és az emberi hibák olyan legkisebb halmaza, amely elegendő egy súlyos baleset előidézéséhez, ha ezek a minimális hibaesemény kombinációban levő meghibásodások együtt, és egyszerre jelentkeznek. [15] [17]

### *CRAMM[1] típusú kockázatelemzés*

A CCTA által kidolgozott módszertan elsősorban az információs rendszerek kockázatkezelésére alkalmas.

Az információs rendszerek biztonságának fogalmát sokféleképpen megfogalmazták. A cikk terjedelme nem teszi lehetővé a variációk felsorolását, itt a véleményem szerinti legpontosabb megfogalmazás: „*A rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. A zárt védelem az összes releváns fenyegetést figyelembe vevő védelmet, a teljes körű védelem, pedig a rendszer valamennyi elemére kiterjedő védelmi intézkedések összességét jelenti. A folytonos védelem az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg*.” [20] A kockázatokkal arányos védelem az, amelynek helyes megállapításához kockázatkezelési eljárást kell végezni.

Az információs rendszerekben a védendő legfőbb érték az adat, amelynek a feldolgozására a rendszert létrehozták. Az adat védendő alaptulajdonságai az adat bizalmassága, sértetlensége és rendelkezésre állása[2] valamint hálózati adattovábbítás esetén a továbbítás letagadhatatlansága és hitelessége. A kockázatelemzés értékelését mindig a fenti tulajdonságok megőrzése szempontjából kell végezni. A tárolt adatok jellegétől függ, hogy melyik a leginkább védendő tulajdonság. Egy minősített, „titkos” adat esetén például a bizalmasság a legfontosabb. Egy törvény adattár esetén a sértetlenség és hitelesség a legfontosabb, bizalmasságot nem is kell biztosítani, hiszen a jogszabályok bárki számára elérhetőek kell, hogy legyenek.

A kockázatelemzés három fő feladatcsoportra bontható, melyek további részfeladatokból állnak.

Az első feladatcsoportban az alapvető szempontok kerülnek megállapításra:

- Meghatározásra kerül a kockázatelemzés hatóköre.
- Azonosításra és értékelésre kerülnek a rendszer vagyonelemei.

A második feladatcsoportban megtörténik a kockázat értékelése a javasolt biztonsági követelmények szerint.

- A rendszerre potenciális veszélyt jelentő fenyegetések azonosítása, a fenyegetések típusának és fokának a megállapítása.
- A rendszer sérülékenységeinek a feltárása, melyeken keresztül a fenyegetés érvényre jutva biztonsági eseményhez vezethet.
- A fenyegetés illetve a sérülékenységi halmaz összevetése, és kockázati értékek kiszámítása szorzással, összeadással, súlyozással, a kockázat értékelő döntése szerint.

A harmadik feladatcsoportban megállapításra kerül, milyen szint feletti kockázatokat kell kezelni, illetve megállapítják azon ellenintézkedéseket, melyekkel az adott kockázatok szintjét az elviselhetőség szintje alá lehet csökkenteni.

## KÖVETKEZTETÉSEK

Végigtekintve a kockázatok elemzésének a történetén látható, hogy a társadalmak, gazdaságok szerkezetének változásával, a termelőerők fejlődésével ez a tevékenység is kiszélesedett. Különböző területek más-más eljárást kezdtek alkalmazni a kockázataik elemzésére. Egyre nagyobb teret kapott a matematika, az elemzéseket tudományos szintre emelve. A kockázatelemzések elkészítésére szakterületenként különböző szoftvereket is

[1] CRAMM - ***C****entral Computer and Telecommunation Agency* ***R****isk* ***A****nalysis and* ***M****anagement* ***M****ethod*

[2] Fogalmak meghatározása a 2013 évi L törvény 1. § (1)

alkalmaznak. Ezek alkalmazása megkönnyíti a munkát, különösen nagy kiterjedésű bonyolult rendszerek esetén, de szem előtt kell tartani, hogy a program nem helyettesítheti az embert, a kockázatelemzésre a vizsgálandó rendszer valamennyi részterületéről szakembereket kell bevonni.

Az információbiztonság területén az információs rendszerek esetében is léteznek szabványok és ajánlások.(ISO/IEC 27001, ISO 31000:2009) Egyik ajánlás sem határozza meg a kockázatkezelés pontos módját.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben rendszerekkel és adatokkal kapcsolatban biztonsági osztályba illetve szintbe sorolást ír elő kockázatelemzés alapján. Új rendszerek tervezésénél, különösen ha minősített adatokat is kell kezelni, kezdeti kockázatelemzést kell végrehajtani. Tehát kockázatelemzés végrehajtása bizonyos esetekben jogszabályban előírt kötelezettség.

A kockázatelemzési módszerek közül információs rendszerek esetében Véleményem szerint a CRAMM típusú kockázatelemzés a legkönnyebben és leghatékonyabban alkalmazható. Jó támpontok lehetnek a vagyontárgyak, fenyegetések, sebezhetőségek előre elkészített listái. Számításai logikusak, nem igényelnek különleges képességeket, ami azért fontos, mert a jogszabályok alapján sok telepítési helyen kell egyszerre elkészíteni az elemzést és a szakemberek ismeretei sem egyformák.

A téma nagysága és cikk méreteinek korlátai miatt az információs rendszerek kockázatelemzésének részletes vizsgálatára nem került sor, ez egy másik tudományos publikáció témája lehet majd.

## FELHASZNÁLT IRODALOM


[1] BODA J. [et al.]: Fókusz és együttműködés. A hadtudomány kutatási feladatai; Honvédségi Szemle 144. évf. 3. szám (2016), 3-19.o

[2] BLESZITY J. [et al.]: Műszaki kutatások és hatékony kormányzás; Hadmérnök 10. évf. 3. szám (2016), 221-242.o

[3] *Hitelintézeti törvény, 14/2001 PM rendelet*.

[4] *Biztosítási ismeretek* – oktatási segédlet, Széchenyi István Egyetem Általános Közgazdasági tanszék, Győr, 2002. 8.oldal

[5] http://privatbankar.hu/fogalomtar?hely=1675&betu=b (Letöltés időpontja: 2017.05.22.)

[6] COSO (2004), *Enterprise Risk Management – Integrated Framework: Executive Summary,* https://www.coso.org/Pages/ermupdate.aspx (Letöltés időpontja: 2017.05.22.)

[7] International Organization for Standardization (2009), *ISO 31000:2009 Risk managementPrinciples and Guidelines*

[8] JENEI T.: *Leggyakrabban használt kockázatkezelési modellek összehasonlítása* [International Journal of Engineering and Management Sciences (IJEMS) Vol. 1. (2016). No. 1.] http://ijems.lib.unideb.hu/file/9/57aa27064359a/szerzo/Jenei.PDF (Letöltés időpontja: 2017.05.22.)

[9] LAWRENCE A. G. és M. LOEB a Marylandi egyetem professzorai (https://www.umd.edu/ )

[10] http://cybervelocity.com/cybersecurity-economics-for-cio-and-ciso/

[11] *Gordon-Loeb Model for Cybersecurity Investments*. https://www.youtube.com/watch?v=cd8dT0FuqQ4 (Letöltés időpontja: 2017.05.24.)

*[12] 370/2011. (XII. 31.) Korm. rendelet 2. § l.*

[13] KERTI A.: *Az információbiztonsági kockázatkezelés oktatásának buktatói*. Kommunikáció 2013. 213 p. (ISBN:978-615-5305-16-0)

[14] *Tansegédlet a veszélyes üzemek szakterületi hatósági feladatok ellátásához.* 12, 35. oldal. kok.katasztrofavedelem.hu/letoltes/document/document_181.doc (Letöltés időpontja: 2017.05.27.)

[15] www.vedelem.hu/files/UserFiles/File/konf2011/KIRVEZ/32_JAGER.ppt. (Letöltés időpontja: 2017.05.27.)

[16] http://www.katasztrofavedelem.hu/letoltes/seveso/szoftverek.pdf (Letöltés időpontja: 2017.05.27.)

*[17] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról, 1. § 2.*

[18] SÁNDOR B.: *A Kockázatkezelés jelentősége* Budapesti Gazdasági Főiskola Budapest, 2011. http://elib.kkf.hu/edip/D_15929.pdf (Letöltés időpontja: 2017.05.28.)

[19] MUHA L.: *Az informatikai biztonság egy lehetséges rendszertana, 2008* [In.: Bolyai Szemle, XVII. évf. 4. szám, p.137-156., Budapest: ZMNE BJKMK, ISSN: 1416-1443]