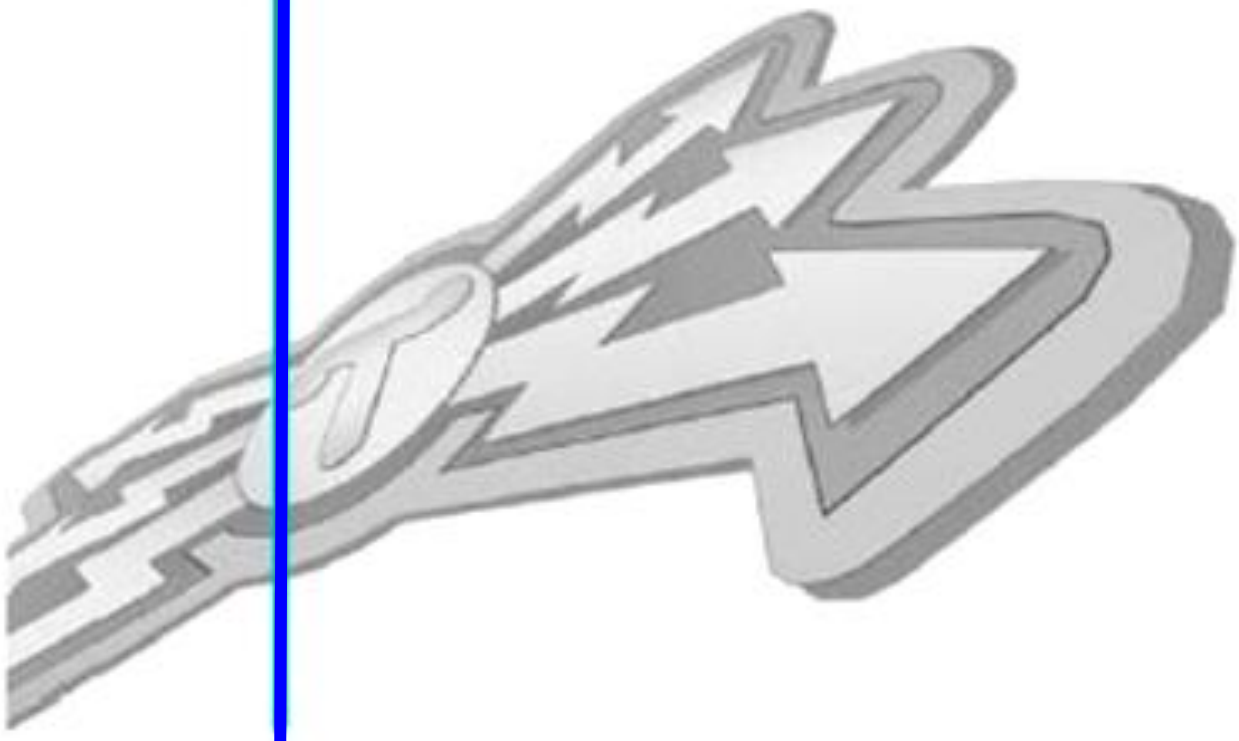
HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos
kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the National University of Public Service

4. évfolyam 2. szám
2013



2013. december 31.

HÍRVILLÁM

a Nemzeti Közszolgálati Egyetem Híradó Tanszék tudományos időszaki kiadványa

SIGNAL BADGE

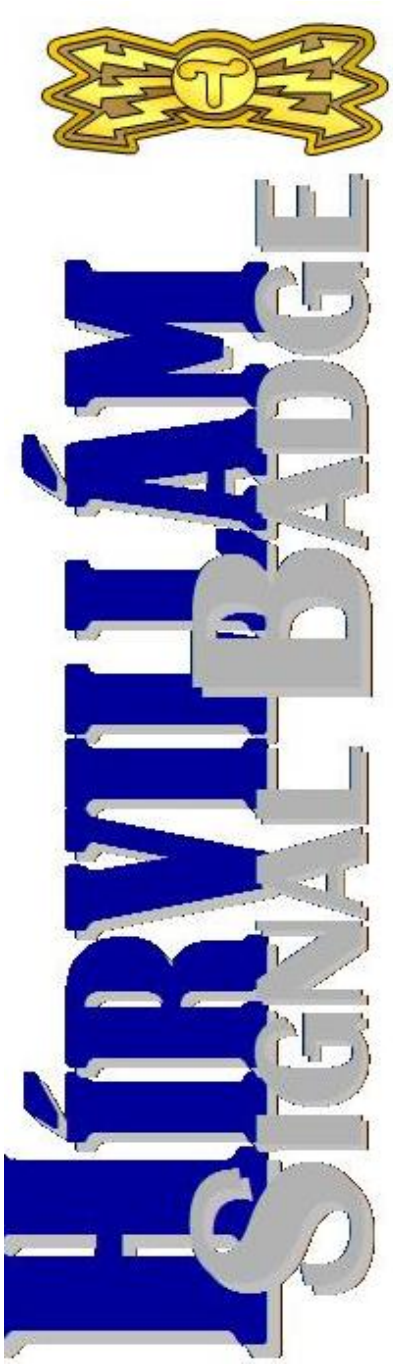
Professional Journal of the Signal Departement at the National University of Public Service

Megjelenik évente két alkalommal

Published twice a year

4. évfolyam 2. szám

Budapest, 2013



Felelős kiadó/Editor in Chief
Dr. Fekete Károly alezredes

Szerkesztőbizottság/Editorial Board

Elnök/Chairman of the Board
Dr. Pándi Erik r. ezredes

Tagok/Members
Dr. Farkas Tibor főhadnagy
Dr. Horváth Zoltán alezredes
Jobbágy Szabolcs százados
Dr. Kerti András alezredes
Prof. Dr. Rajnai Zoltán ezredes
Dr. Szöllősi Sándor ny. őrnagy
Tóth András főhadnagy

Szerkesztette/Co-ordinating Editor
Prof. Dr. Rajnai Zoltán ezredes

HU ISSN 2061-9499

NKE Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15
+36 1 432 9000 (29-110 mellék)

hhk_hirado_szakcsoport@uni-nke.hu

Tartalomjegyzék

Köszöntő

Tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

Rohan az idő és máris eltelt az esztendő. Lezárva az évet ismételten sikeredett szűkös erőforrásaink mellett, igen sok külső segítséggel és támogatással mindkettő szakmai-tudományos konferenciánkat eredményesen – *és megítélésem szerint sikeresen* – megrendezni.

Idén öt fiatal tiszt került a Híradók nagy családjába:

Csombor Csaba hadnagy (MH BHD);
Kun Gergő hadnagy (MH 1. HTHE);
Oláh Dániel hadnagy (MH BHD);
Paráda István hadnagy (MH BHD);
Pfeil Tamás hadnagy (MH BHD).

Büszkélkedhetünk, hiszen a névsorban utolsó három kolléga kiédemelte az NKE HHK által alpított Hadik András Tanulmányi Vándordíjat.

Az ERASMUS mobilitási program keretében lehetőségünk volt két fő – *most már negyedéves hallgató* – saint cyr-i képzésére. Szintén az ERASMUS programnak köszönhetően a külföldi hallgatói részképzés mellett fiatal oktató kollégáink rendszeresen tartottak előadásokat társinmtézményeikben a környező országokban.

Közösségünk tehát kész arra, hogy az újévben továbbra is folytassa oktatási, kutatási és tudományos munkáját szakmai kultúránk elmélyítése és hírnevünk bővítése érdekében.

Mindezen gondolatok jegyében kívánunk Boldog Újévet, illetőleg kellemes időtöltést az idei év második számának áttekintéséhez!

Budapest, 2013. december 31.

Pándi Erik
a Szerkesztőbizottság elnöke

Zele Balázs[1]: Biztonságtechnika erőművi területen. Széntárolási megoldások a hatékony és biztonságos energiaellátás érdekében

Absztrakt

Felgyorsult életünk, és mai világunk kulcsfontosságú kérdéskörei, hogy az emberiség hogyan biztosítja magának az élethez nélkülözhetetlen környezeti feltételeket, továbbá milyen módon kíván a fenntartható fejlődés tudatában biztonságos életvitelt folytatni. Nagyon fontos hogy ugyanúgy, ahogy a mi generációnknak, a jövő generációnak is rendelkezésre kell állnia azoknak a természetben megtalálható erőforrásoknak illetve lehetőségeknek, amelyek a mostani emberiség számára biztosítják a mindennapi életvitelt, a rutinszerű feladatok végrehajtását, melyek már szinte általános érvényűvé és elfogadottá váltak szerte a világban. Jelen tudományos cikkem megírásával szeretném felhívni a figyelmet közvetetten a környezetvédelem, de leginkább a biztonságtechnika fontosságára, melynek egy szeletét tüzetesebben széntüzelésű erőművekben, széntárolási módszerek elemzésével vizsgálom. Ennek megfelelően kitérek a kültéri és fedett tárolási rendszerek előnyeire, hátrányaira és további fejlesztési lehetőségeire, illetve a bennük rejlő alternatívákra egyaránt.

Abstract

The key issues of the world and our hectic everyday lives is how humanity provides itself the life essential environmental conditions, and how it would like to continue its life aware of the sustainable development. It is really important for the future generations to have all the opportunities available in the nature that we have now, which ensure and provide us the everyday life, the implementation of our daily routine, which seem us so natural that we do not always notice it. In this piece of publication I would like to draw attention indirectly to the importance of environment protection and directly to safety technology, which I examine more detailed in coal-firing power plants, through coal storage systems and structures. According to these I write about the topic of inside and covered coal storage structures, and of course I also examine the advantages, drawbacks and future opportunities of these alternatives.

Egy erőmű esetében, amelynek nagyon sok feltételnek és követelménynek kell megfelelnie mind a lakosság, mind pedig a hatóságok felé, górcső alá kell venni a

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola,Ph.D hallgató,, zelebalazs@gmail.com

területen megtalálható környezetvédelmi szempontból veszélyes és nem veszélyes, azaz ártalmatlan anyagok listáját egyaránt. Ezeket fel kell térképezni újra és újra bizonyos időközönként, mert nem elég az erőműtől távolabb eső területekről megállapítani, hogy az ott megtalálható levegő koncentrációs értéke az előírt normáknak és értékeknek megfelel; a létesítmény közvetlen közelében is kifogástalan értékekkel kell rendelkeznie a levegőnek, környezetnek, az erőművi humánerőforrás, a helyi növény és állatvilág szempontjából is. Vizsgálataim széntüzelésű erőművek üzemanyagát hivatott vizsgálni, ezen túlmenően is a szén (mint tüzelőanyag) bányászata és eltüzelése közti intervallumban elfoglalt helyét, méghozzá energiaátalakítási útja során. A széntéren tárolt szenek mennyiségét a kötelező előírásoknak megfelelően homogenizálni kell, hogy megakadályozzák a szén öngyulladási jelenségének kialakulását. Egy erőmű politikáját tekintve ezen fosszilis energiahordozó további nedvességtartalmának növekedésével éri el a folyamat bekövetkezését, amely egyben olcsó és praktikus megoldásnak tűnhet. [2]
Ezeknek a gondolatoknak a megértését és kifejtését szolgálja, hogy nemzetközi forrásokat kutatva, valamint egyéni megállapításokat felhasználva vizsgáljam az ugyan drágább, de hosszú távon kifizetődő lehetőségeket. Egy erőmű dolgozói létszámát, mint biztonságtechnikai és egészségügyi szempontból az egyik legfontosabb tényt figyelembe véve minden lehetséges alternatívát felkutatva kell megtalálni azt a módszert, ami egy eseteleges új technológia alkalmazásával segítheti az erőmű hosszú távú működését. „Kutatásaim során megállapítást nyert bennem az a tény, miszerint a szenet nemzetközi, hazai környezetben is létező különböző okok miatt nagy mennyiségben is tárolhatjuk. Energiapolitikai és stratégiai célokat vizsgálva ezen az okok lehetnek többek között, hogy a nagyobb mennyiségű szén felhalmozása csökkentheti az energiapiaci folyamatoktól való függést, ezzel együtt felkészülést ad olyan üzemzavar, esetleg leállás okozta gazdasági nehézségekre, amelyek a termelés során következhetnek be. A tárolás megvalósítására vonatkozó további okok közé lehet sorolni azt is, amikor enyhébb időjárási és éghajlati viszonyok között kerül sor a kitermelésre, és ezt követően azokon a földrajzi adottságokkal rendelkező területeken épült széntároló létesítmények folytatnak későbbi kereskedelmet, amelyek alacsonyabb környezeti hőmérsékleti tartományokkal rendelkeznek a téli időszakban is. Habár a szénhidrogének ezen fajtájának felhalmozása és tárolása általában nyitott tereken történik, természetesen akadnak zárt terű széntárolási megoldások is. A tárolás időbeli lefolyásától függően csökkenthető a szén nedvességtartalma is, mely a

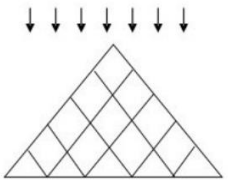
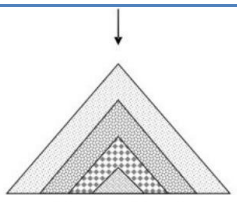
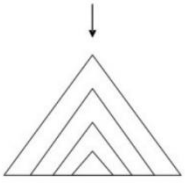
[2] Mátrai Erőmű Zrt. konzultációk, jelentések erőművi dolgozókkal (2013. tavasz)

későbbi tüzelési folyamatok végbemenetelét segíti elő, hiszen nem emésztődik fel plusz energia az energiahordozó eltüzelése, hasznosítása során. Ezáltal az ellátásbiztonságot növelő folyamatról is szót kell ejteni, mint olyan biztonsági metódusról, amely egy széntér mellett létesült erőműnél a folyamatos ellátást hivatott biztosítani. A kitermelt szén leggyakrabban kamionokkal, szállítóvagonokkal kerül elszállításra a bányákban alkalmazott kotrógépektől és a rakodóktól a rendeltetési tárolóegységig. Számos országban különféle tárolási technikákat alkalmaznak erre a célra olyan faktorokat figyelembe véve, mint az éghajlati viszonyok, a tárolók kiterjedése (mérete), építészeti kialakítása és természetesen gépészeti felépítése. Széles körben elterjedt kültéri tároló módszernek számít a Windrow, Chevron és a Cone Shell típusú tárolási rendszer, melyek elvét egy táblázat segítségével foglalok össze. (1. táblázat)"

A Cone Shell típusú tárolási rendszert előszeretettel alkalmazzák nyílt tereken, mivel említést érdemlő hátránya nincs. Egy fedett tároló rendszer kialakításával azonban az 1. táblázatban feltüntetett hátrányok javítását és kiküszöbölését lehetne elérni, méghozzá az időjárásnak kitett szenek nedvességtartalmát lehetne ezáltal csökkenteni, így fedett tárolós rendszereknél ezeknek a lerakási technológiáknak is szerepe lenne, amely további (szerkezeti, technológiai) megoldások alkalmazási alternatívát tenné lehetővé. Emellett az olyan földrajzi területeken, ahol tengeri szállítás útján kerül a széntárolókba a transzportált szén, illetve szeles, esetleg sivatagos területeken működő telepeknél a további időjárásból adódó hátrányokat lehetne megelőzni, ezáltal biztonságos munkavégzést elérni és a környezetkárosító hatásokat (levegő megnövekedett szénpor tartalma) megelőzni.

A tárolás adta pozitív lehetőségek mellett sajnos számolnunk kell a negatív tényezők okozta hatásokkal is. Ahogy az isztambuli egyetem mérnökei is rögzítik, a hosszabb távon szabadon tárolt szén mennyiségeknél az anyag összetételére vonatkozóan különböző kémiai folyamatok beindulása történhet meg (pl. öngyulladás és ebből fakadó tűzesetek). [3]

[3] G. Ökten, O. Kural and E.Algurkaplan (Department of Mining Engineering, Istanbul Technical University, TURKEY), ENERGY STORAGE SYSTEMS – Vol. II – Storage of Coal: Problems and Precautions, (EOLSS)

Rendszer megnevezése	*Windrow (Wöhlbier, 1975)*	*Chevron (Wöhlbier, 1975)*	*Cone Shell (Wöhlbier, 1975)*
Elv	A szénosztályozó homogenizálja a kívánt szénmennyiséget a szemléltető ábra szerint	A szénosztályozó homogenizálja a kívánt szénmennyiséget, méghozzá prizma testekhez hasonló alakban a szemléltető ábra szerint	A szénosztályozó kúp alakban helyezi el a szénmennyiséget a szemléltető ábra szerint
Előny	- Kiválóan homogenizált szénmennyiség - Szállítás utáni kedvező tüzelőanyag minőség	A szén lerakási módja szerint az időjárási csapadék (hó, esővíz, stb.) nem növeli a garmada alsó részein elterülő szén nedvességtartalmát	Téli időjárási körülmények között előnyös alkalmazása, időjárási csapadék mennyisége és nedvességnövelő hatása a legkisebb ebben az esetben
Hátrány	Nyílt tárolás miatt az időjárási körülmények következtében „nedves” szén garmadák létrejötte	Nagyobb széndarabok a garmada felső rétegétől könnyebben elválnak, ezáltal omlási folyamatot indíthatnak el	-
Szemléltető (keresztmetszeti) ábra			

1. táblázat: Windrow, Chevron és a Cone Shell típusú tárolási rendszerek[4]

Az NFPA (National Fire Protection Association) egy publikációjában azonosította a szén szállításával és tárolásával felmerülő veszélyeket, és olyan alternatívát fogalmaz meg, mely alapján védekezni lehet ezekkel a veszélyforrásokkal szemben. Az 1. ábrán egy kupolás szerkezetű – bár ez formailag, és építészeti szerkezetét tekintve lehetne más kialakítású is – építmény létesítésénél megállapítja, hogy tűzvédelmi és biztonságtechnikai szempontból sem készülhet olyan anyagokból ez az építmény, amely veszélyt jelenthet környezetére. Ezeken túl minimalizálni kell

[4] G. Ökten, O. Kural and E.Algurkaplan (Department of Mining Engineering, Istanbul Technical University, TURKEY), ENERGY STORAGE SYSTEMS – Vol. II – Storage of Coal: Problems and Precautions, (EOLSS)

azokat a felületeket az épületen, ahol a finom szénpor megtelepedhet, és ezzel olyan nem kívánatos esetet idézhet elő, amelynek további, akár beláthatatlan következményei is lehetnek (tűzeset, porrobbanás jelensége). [5]

Szabados Gábor Tamás „A természeti adottságok és az emberi tényezők szerepe a bányászati veszélyekben és azok elleni védekezésben" című disszertációjának megfogalmazásában a szénporrobbanás mint jelenség alatt a következőt jegyzi le: *„a levegő keverék olyan heves égési folyamatát értelmezzük, amiben a robbanóképes keveréket a leülepedett szénpor felkavarásával a robbanás önmaga hozza létre és gyújtja meg. A definíció alapján robbanásveszélyesnek azokat a szénporokat tekintjük, amelyek gyújtásátviteli tulajdonságúak."* [6]

Korábbi publikációmban is megjelentek alapján elmondható, hogy „a széntéren tárolt szén mennyiségének különös figyelmet kell tulajdonítani, hiszen nem elég a folyamatos széntartalék biztosítása a további transzportálási és tüzelési folyamatok végbemeneteléhez, a túl nagy mennyiségben tárolt és egymással súrlódási kölcsönhatásba kerülő, valamint a szén tehetetlensége következtében a különböző méretű széndarabok ún. öngyulladása valósulhat meg. Irodalmi vonatkozásban az öngyulladás fogalmán azt a folyamatot értjük, amely külső hőforrás hatása nélkül jön létre.

1. ábra: Kupolás szerkezetű dóm látszati képe, Tajvan[7]

Az anyag a gyulladási hőmérsékletet saját maga hozza létre az anyagban lezajló hőtermelő folyamat eredményeképpen. A folyamat, azaz a felmelegedés történhet

[5] NATIONAL FIRE PROTECTION ASSOCIATION (online), url: http://www.geometrica.com/en/coal-storage-domes (2013. 08. 30.)
[6] SZABADOS GÁBOR TAMÁS, Doktori Értekezés: A természeti adottságok és az emberi tényezők szerepe a bányászati veszélyekben és azok elleni védekezésben, Miskolc, 2011.
[7] NATIONAL FIRE PROTECTION ASSOCIATION (online), url: http://www.geometrica.com/en/coal-storage-domes (2013. 08. 30.)

vegyi reakció (pl.: szén telítetlensége), vagy biológiai mikroorganizmusok útján. A felmelegedés folyamán az anyag, jelen esetben a lignit elérheti az öngyulladási hőmérsékletet. Ezen okokból kifolyólag a széntéren tárolt lignitet pl.: a nyári forróságok idején, kiépített vízpermetező rendszerrel hűtik, hogy ne következhessen be az öngyulladási hőmérséklet elérése és ezzel a tűz folyamatának beindulása." [8]

„Ezt támasztja alá a szénpor vizsgálatára alkalmazott Glivitzky-féle próba is. Ez egy tapasztalati tényezőkre alapozott vizsgálat, amely szerint, ha egy efféle anyag 150°C-on vagy ennél alacsonyabb hőmérsékleten képes meggyulladni a próba során, abban az esetben normál körülmények között öngyulladó anyagról van szó. Azonban ha ez a hőmérsékleti tartomány 180°C, vagy akár ennél nagyobb hőmérsékleten megy végbe, nem kell az öngyulladás folyamatával számolni. Ahogy azt a Dr. Simon Ákos-Török László E. Alkalmazott Kémia c. könyv is megfogalmazza, az anyagban fellépő hőfejlődési sebességet csökkentve, vagy a frissen kibányászott szenet pl. a Mátrai Erőműben is alkalmazott módon, a széntéren betároljuk, és szellőztetjük, azaz „öregítjük". Ennek oka, hogy a szén idővel „passziválódjon", vagyis a levegőadszorpció csökkentési cél elérhető legyen. Másik fontos tényező, hogy az anyagot a lehető legkisebb hőhatásnak kitett módon tartsuk. Gazdasági szempontból, és hőfejlődés kialakulás céljából is megfelel az erőmű területére a bányákból, a szalagrendszer által beérkező szén betárolása, ugyanis az év nagy részében Magyarország éghajlatának köszönhetően kevés azon hónapok száma, amikor nagyobb mértékű hőmérsékletingadozásnak lenne kitéve a lerakott szén/lignit. A szénre nézve a korábban már részletezett módon oldják meg az ezen időszak által okozott hőmérsékletmegnövekedési-hatásokat." [9]

Ki kell tehát dolgozni egy olyan alternatív megoldást, mely minden lehetséges eshetőségre megoldást kínál, és további veszélyek, többek között a nem kielégített energiaszükségletek bekövetkezését is kizárja.

Ebben az olvasatban, az NFPA cikk javaslatai szerint (is) célszerű kerülni a szén vízi permetezéses eljárását, leginkább tűzvédelmi szempontok alapján, bár ahogy más erőműveknél is gyakori, úgy a magyarországi lignittüzelésű Mátrai Erőműben is alkalmazzák ezt az eljárási módot. Alapja, hogy a szén öngyulladási jelenségének kialakulását megfékezzék, másrészt a széntérről az erőmű területén lévő közútra kerüljön a finom szemcsenagyságú lignitpor, mely aztán később az időjárási, vagy egyéb környezeti hatásra akár az emberi szembe, tüdőbe kerüljön. Érdemes nem

[8] Zele Balázs, A tűz kezelés erőművi berkekben, tudományos közlemény, Szolnoki Tudományos Közlemények XVII. Szolnok, 2013.
[9] Dr. Simon Ákos-TÖRÖK LÁSZLÓ E., Alkalmazott Kémia. 30/2008.

csupán az emberre vett hatást vizsgálni, de a környezetre, a gépi berendezésekre vett kihatásukat is szemügyre venni, és ezeket elemzésekkel alátámasztani, hiszen fontos, hogy milyen szemcsenagyságú szénpor okozhat eltömődéseket műszaki berendezések forgó, vagy egyéb alkatrészeiben.

A széntároló csarnok elemzéséhez visszatérve egy lehetséges konstrukció megépítést követően további vizsgálatok folytatódnának. Termodinamikai szempontból, és ahogy a már említett leírás is foglalkozik a kérdéskörrel, folyamatos mérési sorozatok elvégzése lenne szükséges, elsődlegesen a hőmérséklet alakulása és változása céljából. A széntároló csarnok tartópilléreinél, és azokon a helyeken, ahol a szerkezet kivitelezésétől függően kisebb-nagyobb terhelési pontok keletkeznének, eleinte próbaméréseket, majd rendszeres méréseket lehetne végezni. Tűzvédelmi biztonsági rendszerek kialakítása is növelné a biztonságos tárolási módot, amit erőművi fennhatóság alá tartozó tűzoltóság felügyelne.

„Szakirodalmi vonatkozásban a tűzvédelem témakörébe tartozik a tűzesetek megelőzése, a tűzoltási feladatok teljesítése és ellátása, továbbá a tűzvizsgálatok (okok feltárása, esetek bekövetkezési mivolta), mint hatósági tevékenység a 44/2011. (XII.5.) BM rendelet alapján.” [10]

Véleményem szerint amennyiben a fent megjelölt megoldás lehetséges, olyan rendszerben kellene a széntömeget tárolni, hogy egy esetleges lángra lobbanás jelenségénél azonnal el lehessen távolítani az adott mennyiséget, vagyis cellákra, tárolókra kellene osztani a széntér területét, továbbá a szakirodalmi megfogalmazások alapján a nem fedett tárolós eljárásoknál is alkalmazott eljárási modulokat lehetne működtetni. Az erőmű más területein is alkalmazott oltási módok és rendszerek kiépítésével biztonságossá és az azonnali beavatkozás lehetőségének biztosításával a kiépülő struktúrát közel maximális mértékben kockázat és balesetmentes területté lehetne nyilvánítani.

A munka és egészségvédelem köre, ami a biztonságos munkavégzés folytatásához szükségeltetik, fontos szerepet kap mindennapjainkban. A munkahelyi veszélyek és balesetek elkerülése érdekében folyamatos fejlesztésekre van szükség, hiszen a legnagyobb erőfeszítések ellenére is számos eset lehetséges, ami ezen események (veszélyek) sorozatát hordozza magában. A biztonságos munkavégzés növelésének

[10] Dr. Szabó Gyula – Dr. Szűcs Endre: Munkavédelem a szakképzésben, Egyetemi jegyzet, , Óbudai Egyetem Budapest 2012.
http://www.ommf.gov.hu/nyomtatvanyok/MV.kiadv.munkavedelem.szakkepzesben.pdf (2014. 01. 05.)

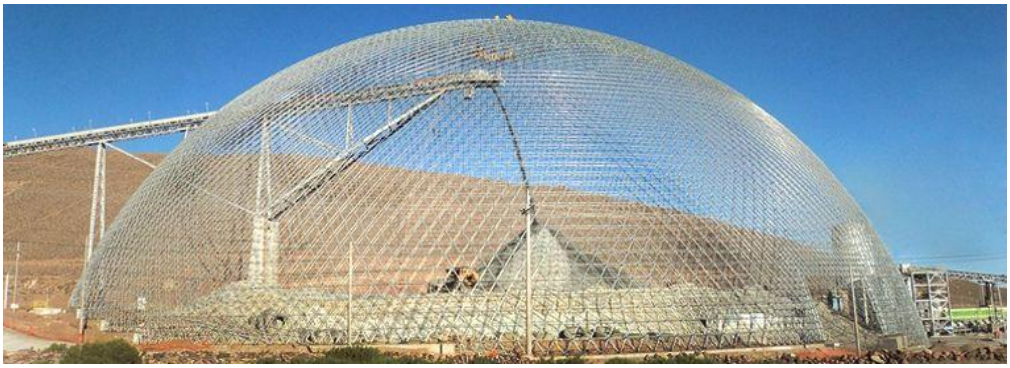
biztosítására folyamatosan vizsgált és fejlesztés alatt álló munkavédelmi ruházat, továbbá kiegészítő eszközök (munkavédelmi szemüveg, hallásvédő stb.) állnak rendelkezésre a minél kevesebb baleset és veszélyek elkerülése céljából. Ezen kockázatok folyamatos redukálása érdekében és a további biztonsági hatékonysági mutatók növelésével (zárt széntároló kialakítása) tovább lehetne növelni a biztonságos munkavédelmi körülmények létrejöttét.

Cikkem elkészítése közben, valamint látóköröm szélesítésével további, eddig még ezen a területen megoldatlan alternatívák fogalmazódtak meg bennem. Különböző erőművi szerkezeti felépítéseket tekintve magyarországi viszonylatban, erőművi léptékben is mérhető idősebb építési kivitelezésekről lehet beszélni, így a szükséges üzemidő-meghosszabításokon túl, idővel újabb beruházások lesznek aktuálisak. Ezt a megállapítást támasztja alá többek között Dr. Stróbl Alajos „Építsetek erőműveket" címmel megjelent tudományos közleménye is, melyben az aktuális hazai energiapolitikai helyzetet vizsgálva állapítja meg, hogy *„az adott országban szükség van új erőművekre, kicsikre és nagyokra egyaránt. Ebben az országban is elsősorban a következő évtizedben kell sok erőművet építeni, mint Európában, vagy Németországban."*[11] A leállítások sebességétől, a gazdasági, környezetvédelmi és jogi kényszerektől teszi ezeket függővé, melyből egyértelműen nem lehet kijelenteni, hogy szenes erőművek működésére ne volna szükség hazánkban. [12] Gondolatait követve, *„nincs más hátra, mint az erőműépítés: kezdetben a sok kicsi, majd a leállások megindulásával gázturbinás nagyok, a következő évtizedben pedig ismét jöhetnek a menetrendtartó szénerőművek."* [13]

Számos olyan terület van a szenes technológiára épült (így napjainkban már elöregedőnek tekinthető szenes erőműben/erőművekben) létesítményekben, akár a blokkokon belüli állapotokat vesszük figyelembe, akár az üzemi területet, ahol a technológiai szempontból is adódóan, de álláspontom szerint nem megoldhatatlan jelenséggel állunk szemben. Abban az esetben például, ha a bánya vonzáskörzetében helyezkedik el az erőmű, előfordulhat, hogy a szén és szénpor a széntérről szállító szalag rendszeren jut el a kazánokig. Ezek a rendszerek technológiailag fedett és leburkolt berendezések, amelyek többek között megakadályozzák a szénpor irányítatlan és nem kívánatos eloszlását az üzem területein belül. Azonban ha mégis megtörténik ez a szabályozatlan eloszlás (bekövetkező tűzeset a szállító rendszerben), azt természetesen mihamarabb orvosolni kell. A mai állapotok szerint egyes erőművek a szállítás utáni tárolási

[11] Dr. Stróbl Alajos, Építsetek erőműveket!, tudományos közlemény, MAGYAR ENERGETIKA, (2003/6)
[12] u.o.
[13] u.o.

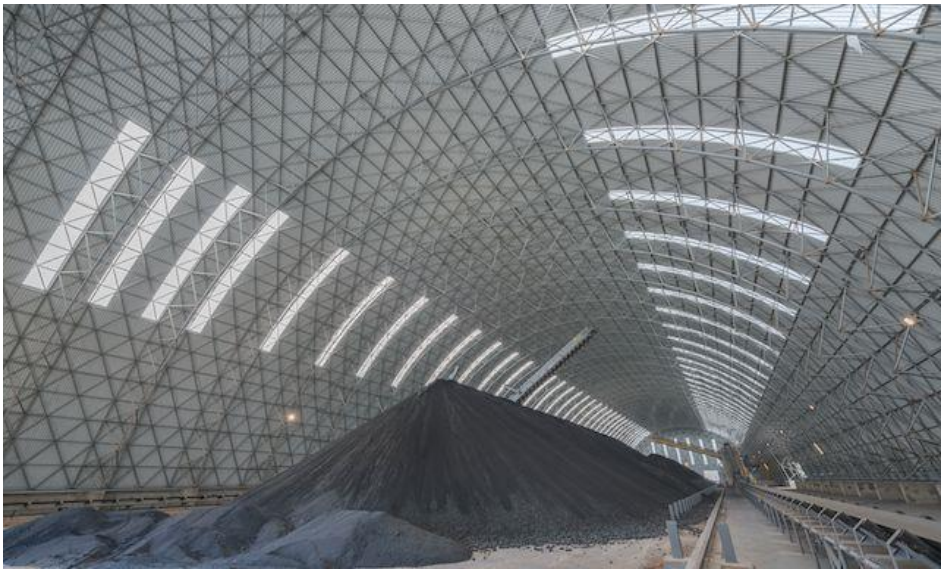
fázisnál többnyire humánerőforrás/emberi erő bevonásával próbálják meg minél nagyobb mértékben lecsökkenteni a lignitpor technológiailag szabályozatlan helyre való eljutását. A széntároló terület lefedésének megvalósításával tehát további kényes kérdések kerülhetnek megválaszolásra, egyúttal emberi tényezők (hibák) vonhatóak ki a rendszerből.
A kialakításnak biztosítani kell egy olyan területet, ahol egy portalanító rendszer beépítésével összegyűjtött por mennyiségét tárolni lehet, és később ezt további hasznosításra fel lehet használni. Szintén egy másik területhez is kapcsolódhat ez a portalanító és összegyűjtő rendszer kivitelezésének tervezete, ugyanis az erőművek más területeinél felgyülemlett pormennyiséget is hasonló módon kellene összegyűjteni és tárolni. Meg kell szüntetni azokat a réseket és olyan kialakítású területeket, ahol a finom porszemcse megragadhat és összegyűlhet. Ezeken túlmenően biztosítani kell olyan szellőző rendszer kiépítését a kupolán belül, amely meggátolja a porrobbanás és egyéb tűzesetek kialakulását.
A szerkezeti kialakításokon és változtatásokon túl, illetve ezeket megelőzően, a korábbiakban tárgyaltak szerint az emberre nézve mérgező (káros) anyagnak tekinthető (szálló szénpor) koncentráció mértékéről és eloszlásáról egy új, tudományos mérési sorozatából még alaposabb és pontosabb eredményt lehetne felmutatni, mint ezen anyagok fizikai elven működő kimutatására alkalmazható berendezések bevonásával.
A következő ábrán egy korábban már megépített konstrukció bemutatásával szemléltetem a megvalósított létesítményeket.



2. ábra: Széntároló csarnok megvalósítási terve[14]

[14] GEOMETRICA hivatalos honlapja (online), url: http://geometrica.com/bulk-storage (2013. 12. 29.)

3. ábra: Széntároló csarnok megvalósítási terve (Florida)[15]



4. ábra: Széntároló csarnok megvalósítási terve (Tunézia)[16]

Jól érzékelhető a világ különböző területein megépült berendezések ábráiból továbbá a bemutatott tanulmányok alapján is, mennyire fontos kérdéssel állunk szemben, ami a környezet megóvását, a biztonságos és zavartalan energiaellátás megvalósítását illeti.

[15] GEOMETRICA hivatalos honlapja (online), url: http://geometrica.com/bulk-storage (2013. 12. 29.)
[16] u.o.

Összegzés

Összefoglalásként elmondható, hogy a tűz- és környezetvédelem, a biztonságtechnika tudománya mára szoros együttes működési rendszert alkot, melyet jól szemléltet a világ különböző pontjain elhelyezkedő széntüzelésű erőművek közvetlen és közvetett területeit érintő káros anyag (szénpor) együttes eloszlási rendszerének kérdésköre és ehhez mérten az emberi és mérnöki felelősségvállalási architektúra. Elemzésem során bemutattam a már alkalmazott széntárolási technológiák rendszerét és felvetettem a vonzáskörzetüket érintő szénpor koncentrációs megoszlási folyamatokat. A széntárolási technológiáknál kitértem a kültéri és a fedett tárolós megoldásokra egyaránt; a kültéri tároló lehetőségeket vizsgálva azonban annak hátrányait latba véve egy, a külföldi forrásokat és példákat követő fedett tároló struktúrát javasoltam kialakításra. Ezek mellett felvetettem a megoldatlan környezeti károkat is előidézhető veszélyforrások megelőzésére alkalmas rendszerek alternatív lehetőségeit – akár a kialakult tűz okozta, akár a megnövekedett szénpor koncentrációs értékeket keltette károkról legyen szó. Ezeken túlmenően további fejlesztési irányokat határoztam meg, melyek a jövőre tekintve újabb mérnöki megoldatlan gátak áthidalását lesz hivatott megoldani.

Summary

All in all as a summary, we can say that the environment protection and the science of safety engineering now forms a close co-operation system, which is shown clearly in the question of the dust concentration near and indirect district of different coal-powered plants and also in human and engineering collective responsibility all around the world. During my publication I examined the dust and lignite-dust concentration near the power plant and its suburban area. At the topic of coal storage technology I wrote about the outside and the covered storage systems as well; however examining the outside systems and their disadvantages and taking into consideration some foreign resources and options I suggested a covered storage opportunity to create. Besides this, I mentioned a useable alternative possibility to prevent hazardous facts which may cause – so far – unsolved environmental damages – whether caused by a fire accident or the increased coal dust concentration. In addition to this, I determined further development directions in the future, which may lead to solve these unresolved engineering barriers.

Felhasznált irodalom

1. **NATIONAL FIRE PROTECTION ASSOCIATION (online),** url: http://www.geometrica.com/en/coal-storage-domes (2013. 08. 30.)
2. **G. Ökten, O. Kural and E.Algurkaplan,** (Department of Mining Engineering, Istanbul Technical University, TURKEY), ENERGY STORAGE SYSTEMS – Vol. II – Storage of Coal: Problems and Precautions, (EOLSS)
3. **ZELE BALÁZS,** A tűz kezelés erőművi berkekben, tudományos közlemény, Szolnoki Tudományos Közlemények XVII. Szolnok, 2013.
4. **DR. SIMON ÁKOS-TÖRÖK LÁSZLÓ E.,** Alkalmazott Kémia. 30/2008.
5. **SZABADOS GÁBOR TAMÁS,** Doktori Értekezés: A természeti adottságok és az emberi tényezők szerepe a bányászati veszélyekben és azok elleni védekezésben, Miskolc, 2011.
6. **Mátrai Erőmű Zrt. konzultációk,** jelentések erőművi dolgozókkal (2013. tavasz)
7. **GEOMETRICA hivatalos honlapja (online),** url: http://geometrica.com/bulk-storage (2013. 12. 29.)
8. **DR. SZABÓ GYULA – DR. SZŰCS ENDRE,** Óbudai Egyetem: Munkavédelem a szakképzésben, Egyetemi jegyzet, Budapest 2012. (online), url: http://www.ommf.gov.hu/nyomtatvanyok/MV.kiadv.munkavedelem.szakkepzesben.pdf (2014. 01. 05.)
9. **DR. STRÓBL ALAJOS,** Építsetek erőműveket!, tudományos közlemény, MAGYAR ENERGETIKA, (2003/6)

Szabolcs Hullán*[17]*: Safety assessment of events

Absract
The assessment of unplanned events in a nuclear facility is of crucial importance with regard to operational experiences. The assessment of the event may indicate certain deficiencies, the removal of which is essential for safe operation. The Hungarian regulatory body have been developed an event-assessment method that is used to determine the safety relevance of the event. The method is based on a detailed investigation of the events. During the course of this investigation proper information must be collected factors of safety must be addressed based on values specified earlier. Each event is designated by a figure, which indicates the safety level of the events (the higher the total score, the more serious the safety relevance is). This assessment methodology quantifies the features of safety culture and human factors according to events.

1. The safety assessment of nuclear events

The quantification of the level of safety is a quite difficult task for all industry sectors. The calculation of the quantity of relation of the safety, or the safety level would be very important for operator and regulator. However it is not an easy opportunity. The following description aims to show an event, which occurs in the nuclear installations, assessment method of the Hungarian regulators.
The assessment of design basis events or potential design basis events is somehow similar to the rating according to International Nuclear Event Scale (INES) but the INES rating method is – in my opinion – more subjective in the topic of "smaller safety significant events". Of course the INES rating is classified according to safety significance, but the purpose of the classification is different. The INES rating is important in the public communication point of view, the following event assessment method is important for the safety.
At the assessment of the events is quit important the characteristics of the safety culture and the human factor. This following method gives priority to these aspects.

It is important for the carry out the event assessment method to available all relevant and necessary information. Indeed, the assessment is based in

[17] Óbudai Egyetem Biztonságtudományi Doktori Iskola Ph.D hallgató

information which comes from the detailed investigation. So we need all safety connected data for the safety related features. According to method all features have had been established with their “sub features” and they have had been bound with numerical values. All features must be evaluated separately and must be determined the characteristic numbers. These values have to be summarized and they are given the level of the safety significance of the event. In this case for each event has its own value, which indicates its relative safety level. The highest score of the event is the most serious in nuclear safety point of view (including human factors and safety culture). The method does not capable for determination of absolute value of the events, but the method makes comparable these events in safety significant point of view.

2. The features and their characteristics

As far as possible the subjectivity was excluded the determination and divided of the subfeatures. 10 features were identified and they were divided subfeatures, and the subfeatures have an own values. The features are the following:

1 Initial event
2 Reactor scram
3 Violation of Technical Specification (TS)
4 The functionality of operating staff
5 The risk of the core melt frequency
6 The causes of event
7 Other features of the event
8 Safety classification of the event related systems, structures and components
9 The received dose of the staff
10 Radioactive release

The listed characteristics are very different, the uniforming of their assessment is difficult. Therefore, the characteristics of different groups should be listed.

a) There are the "two-state" features (it occurs during event or not). It includes:
   - Initiating events (real and potential)
   - Reactor scram
   - Violation of TS
   - The functionality of operating staff
   - Other features of the event (common mode failure, common cause failure, recurrent event, poor safety culture, design basis, problem of

safety analysis, complete or partial degradation of related safety functions)
- The received dose of the staff
- Radioactive release

b) a few additional features can be added a defined or calculated value:
- The risk of the core melt frequency
- The causes of event
- Safety classification of the event related systems, structures and components

c) there are further features that are important their magnitude:
- The received dose of the staff
- Radioactive release

3. Assessment of the safety culture

The quantification of safety culture is also difficult. However, the method provides an opportunity to compare the events year-on-year in safety culture point of view. Therefore the different values of the following features can be analyzed and compared (e.g. as part of the annual assessment):

- Violation of TS
- The functionality of operating staff
- Recurrent Events
- Event caused by design failure
- The received dose of the staff

4. Designation of the scores for events

Let's look at examples of two subfeatures and their values!

Initial event

The initial event is an identified event that leads to anticipated operational occurrences or accident conditions. This term (often shortened to initiator) is used in relation to event reporting and analysis, i.e. when such events have occurred. For the consideration of hypothetical events considered at the design stage, the term postulated initiating event (PIE) is used. The initial event identified during design as capable of leading to anticipated operational occurrences or accident conditions. The primary causes of postulated initiating events may be credible equipment failures and operator errors (both within and external to the facility) or human induced or natural events.

First of all it has to decided whether there was a real initial event or not. It is clear that a real event fall under serious consideration, as the failure (event) comes into light during a planned test or inspection and there was no real initial event. However, for the assessment of the event has to be taken into account the likelihood of the relevant initial event. The quantifications of the features are the follows:
In case of real initial event value is 4, the absence of a real initial event: 1. for the designation of the numerical values of the event must be considered the safety relevant of initial event.

	Subfeatures	**Value**
1.	There was no real initial event (potential only).	1
2.	There was an initial event.	4
3.	The frequency of real or potential initial event: expected (> 2 × 10-2).	1
4.	The frequency of real or potential initial event: possible (2 × 10-2 <x <3 × 10-4).	2
5.	The frequency of real or potential initial event: unlikely (<3 × 10-4).	3
		Σ=2÷7

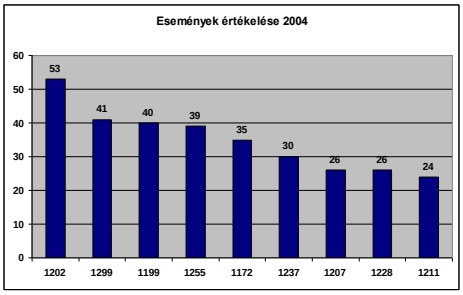
5. Technical Specification (TS) violation

The described two features "two-state" features (it occurs during event or not). For the assessment this features – considering the human factor – is very important that the violation is deliberate or undeliberate (see table 2). The determination of the deliberation is a very hard problem, because in most cases there are not real evidence of it. The deliberate violation of TS is the most dangerous that justifies the highest scores.

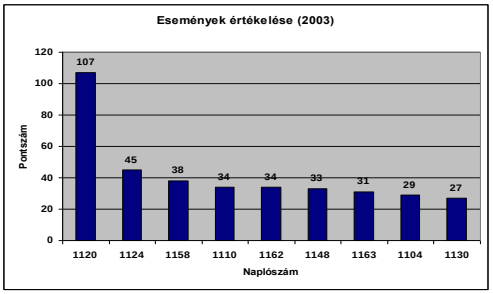
There could also be communicated further details, but the detailed description of this method could not be possible in frame of this article.

	Subfeatures	Value
1.	TS was not contacted.	0
2.	TS was contacted.	1
3.	There was a violation of TS but the operational staff abolished the violation hence they have just discovered it.	6
4.	TS violation (undeliberate)	8
5.	Technical Specification Violation (deliberate)	12
		Σ=0÷12

6. Results



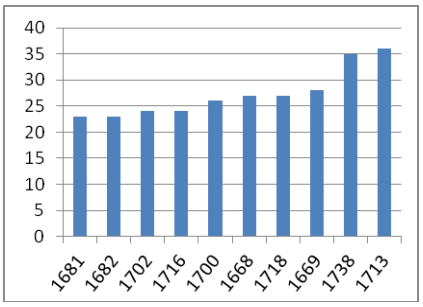
1. figure: result of events in 2004



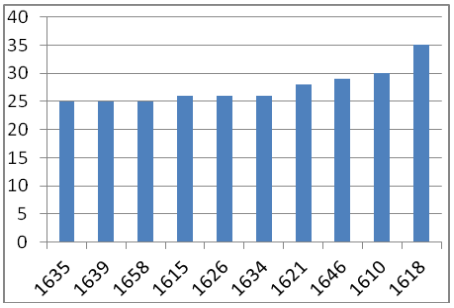
2. figure: result of events in 2003

30 fuel elements damaged in the cleaning tank in 2003 in the Paks NPP that is why the year 2003 and the further two years are presented. The next two diagrams show the results of event assessment in last two years (2011, 2012). The events marked by the HAEA registration number.

The above mentioned highest score of the event can be seen on figure 4 (1120). This event got the most features It is clear that there were in addition to some more serious events in the year 2003 (1110, 1104). After the finishing of the comprehensive action plan which was recommend supplemented by the international mission and was prescribed by the regulatory body the scores were reduced and there are in the same level at present as well (see on figure 1,2,3,4).



3. figure: result of events in 2011



4. figure: result of events in 2012

Summary

With several years of practical experience has shown that the method is a useful tool for nuclear safety assessment. The advantage of this methods:

- one more tool for safety assessment of events,
- it quantifies the certain events of safety relevance,
- it is objective as far as possible, and
- it could give a picture about safety culture and human factor of the events.

Disadvantages of this assessment method:

- the given scores for events don't indicate the real or absolute level of safety,
- The scores of the events could be compared only each other so this is a relative assessment opportunity,
- direct corrective actions don't initiate based on the results of this assessment.

Although, the one of the most important role of this assessment tool is to discovering the early signs of the degradation of nuclear safety in the nuclear facilities.

References

[1] Assessment the unplanned events in nuclear facilities, ETM Ltd., 2002
[2] IAEA Safety glossary edition 2007.
[3] Dr Rajnai Zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23., 2010
[4] The safety assessment of the Hungarian nuclear facilities 2012, HAEA.
[5] The safety assessment of the Hungarian nuclear facilities 2011, HAEA.
[6] The safety assessment of the Hungarian nuclear facilities 2004, HAEA.

[7] The safety assessment of the Hungarian nuclear facilities 2003, HAEA.
[8] Events safety assessment (ME-3-0-18 HAEA procedure), 2005

Mógor Tamásné - Rajnai Zoltán: [18] ***Elektronikus adatkezelő rendszerek kockázatelemzése, kockázati módszerek bemutatása, összevetése***

Absztrakt
A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.
Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.[19]

Abstract
The interest of national priority - because of threats to today's information society - national electronic data assets as part of the national wealth, and this management information systems and the security of critical information systems and system components.
Social expectations managed electronic information systems is essential for the state and its citizens, data and information confidentiality, integrity and availability. Constituents integrity and availability of closed, ensuring complete and continuous protection commensurate with the risk, thereby protecting cyberspace.

1. Alapok

Az információ megszerzése és védelme ősidők óta foglalkoztatja az emberiséget. Ez a tevékenység az emberi társadalmakkal alakult ki és fejlődött. A kezdetleges számítógépek megjelenésekor, majd később a fejlett, adatkezelő rendszerek kifejlesztésével az információ megszerzésének és védelmének jelentősége, módja is megváltozott.
A 19. század végétől kezdve olyan dinamikus változások kezdődtek az egész világon, melyek az élet minden területén gyors fejlődést, átalakulást eredményeztek. Gondoljunk csak a közlekedés, híradás, energetika területére, melyek rendkívüli

[18] Óbudai Egyetem Biztonságtudományi Doktori Iskola Ph.D hallgatója (mogor.tamasne@uni-nke.hu), OE egyetemi tanár
[19] 2013. évi L. törvény bevezető rész

változást hoztak az emberiség életében, ugyanakkor sérült az egyén, a közösségek, nemzetek, országok, vagyis az egész világ biztonságérzete. Az ember nem tudta felvenni azt a dinamikát, amit a fejlődés diktált. A túlzott gyors és hirtelen fejlődés helyett lassú, szerve, kidolgozott folyamat lenne ideális.) Az 1900-as évek közepétől pedig egyre jelentősebb szerepet kapott a biztonság kérdése.[20]
A biztonság magas szintje csak korszerű védelmi, biztonságtechnikai rendszerekkel valósítható meg. Az elvárt biztonsági szint egyre növekszik, mivel a biztonságtechnikai rendszerek egyre bonyolultabbá válnak. Az integrált, komplex biztonság a magas biztonsági szint elérésének alapvető követelménye, hogy figyelemmel kísérjük az adott rendszert, feltárjuk, elemezzük a kockázatokat, melyek veszélyeztetik a rendszer működését. Ezután próbáljuk a kockázatok szintjét és mennyiségét úgy lecsökkenteni, hogy a lehető legbiztonságosabb működést érjük el.

Ebben a folyamatban van egy szerves alkotóelem, aki maga az EMBER, hiszen ő a biztonság megteremtője és fenntartója.
Az Amerikai Egyesült Államokban már az 1970-es években teret hódított az információbiztonsági értékelés következetes rendszerének kidolgozása, előtérbe helyezése. Idővel mindez átterjedt Európába, Magyarországon pedig 1996-ban kapott jelentősebb szerepet, amikor a Miniszterelnöki Hivatal hazai ajánlást adott ki Informatikai Rendszerek Biztonsági Követelményei címmel.
A 2001. szeptember 11-én történt események megerősítették azt az elvárást, hogy a szakembereknek fel kell készülniük a legváratlanabb eseményekre. Sajnos a veszélyek és kockázatok növekedése egyre hangsúlyosabb szerepet szán olyan tevékenységeknek, mint a kockázat, megelőzés, védekezés, védelem, biztonság. Az EU 2002/43-as határozata arra késztet, hogy minden ország – *ahol ez lehetséges* – indítson információs oktatási kampányokat annak érdekében, hogy az információbiztonság egységessé, nemzetközileg elfogadott szabályozáson alapulóvá váljon, amely az elmélet és gyakorlat szintjén is megalapozott, alátámasztott legyen.

2. Alapfogalmak

Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;
Adatfeldolgozás: az adatkezeléshez kapcsolódó technikai feladatok elvégzése;

[20] Biztonság: komplex fogalom, egy folyamatosan változó helyzet fokmérője, az egyén, társadalom komfortosságának fokmérője.

Adatfeldolgozó: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelő részére adatfeldolgozást végez;
Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása,
Adatkezelő: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaságegyéni vállalkozó, aki vagy amely az adatkezelést végzi;
Auditálás: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;
Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;
Biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;
Biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;
Biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége;
Biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;
Elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;
Életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;
Fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei

védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

Fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;

Folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;

Globális kibertér: a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;

Informatikai biztonságpolitika: a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;

Informatikai biztonsági stratégia: az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;

Információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti,

Kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez;

Kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;

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

Kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

Kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével;

Korai figyelmeztetés: valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;
Logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;
Maradványkockázat: az a tudatosan felvállalt kockázat, amely alapvetően – kis mértékben – annak ellenére is fennmarad, hogy a fenyegető tényezők ellen intézkedések eredményesen végrehajtásra kerültek.
Megbízható működés: az informatikai rendszerek, és az általuk kezelt adatok által hordozott információk rendelkezésre állásának és funkcionalitásának védelme.
Megbízhatóság: a megbízhatóság műszaki értelemben egy informatikai rendszerelemnek vagy rendszernek az a jellemzője, amely megadja, hogy az üzemeltetési feltételek fenntartása esetén milyen mértékben várható el annak hibátlan, rendeltetésszerű működése.
A megbízhatóság matematikai értelemben egy statisztikai fogalom, amely annak a valószínűségét adja meg, hogy egy rendszerelem, vagy rendszer jellemzői az előírt határok közé esnek.
Meghibásodási tényező: az informatikai rendszer (vagy rendszerelemek) megbízhatóságát jellemző olyan mutatószám, amely megadja, hogy adott időpont után, kis időegységen belül, az informatikai rendszerelemnek mekkora a meghibásodás valószínűsége, feltéve, hogy az adott időpontig az eszköz nem hibásodott meg.
Megelőzés: a fenyegetés hatása bekövetkezésének elkerülése;
Reagálás: a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;
Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;
Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer
eleme rendeltetésének megfelelően használható;
Sérülékenység: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

Számítógépes incidenskezelő Központ: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];
Szervezet: az adatkezelést vagy adatfeldolgozást végző jogi személy, valamint jogi személyiséggel nem rendelkező gazdasági társaság, egyéni vállalkozó;
Támadás: valamely személy (tettes) akciója azzal a szándékkal, hogy valamely informatikai rendszert veszélyeztessen és károkat okozzon.
Teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;
Üzletmenet folytonosság tervezés: az informatikai rendszerrendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek. (BCP – Business Continuity Planning)
Veszélyforrás: ide sorolható mindaz, aminek támadás formájában történő bekövetkezésekor a rendszer működésében nem kívánt állapot jön létre, illetve az erőforrások biztonsága sérül.
Védelmi intézkedés: a fenyegetettség bekövetkezési valószínűsége, illetve a bekövetkezéskor jelentkező kár csökkentésére szervezési vagy technikai eszközökkel tett intézkedés.
Védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;
Zárt célú elektronikus információs rendszer: jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer;
Zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

3. A kockázatmenedzsment, mint a biztonság alapja

A bevezetőben már említettem, hogy a kockázatmenedzsment előtérbe helyeződése elsősorban a technika rendkívül gyors fejlődésének köszönhető.
Napjainkban a szervezetek sikeres működése már szinte lehetetlen informatikai eszközök használata nélkül. Az elmúlt 25-30 évben az informatikai rendszerek életünk szerves részévé váltak. Jelen vannak a magán, állami, védelmi, üzleti szférában, és egyre inkább kitüntetett szerepet kapnak.

Az informatikai rendszer védelme minden esetben a szervezet vezetésének a felelőssége és ez a felelősség nem átháríthatóan (azonban megfelelő körülmények biztosítása esetén delegálható). A szervezet külső szervezeteket is megbízhat (pl.: kiszervezés keretében) a védelmi rendszer kialakításával, működtetésével és a működés ellenőrzésével, de a teljes kontrollkörnyezet megfelelőségének biztosítása ez esetben is a vezetőség feladata marad.
Az IT rendszerek központi szerepe és sérülékenysége miatt napjainkban elengedhetetlen az informatikai rendszereket fenyegető veszélyek feltérképezése, és a kockázatok megfelelő kezelése, menedzselése. A szervezetnek ki kell alakítania a tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.

Egyes felmérések[21] szerint a vállalati vezetők 60%-a évente minimum 1 incidensre számít, 5 évente pedig minimum 1 súlyos adatvesztéssel járóra.
A kockázatelemzés eredményeként kidolgozhatók a megfelelő védelemhez szükséges kockázatkezelési stratégiák. Az IT kockázat menedzsment programok kialakítása során figyelembe kell venni a szervezet specifikus kockázati profilját, üzleti céljait, az újabb kockázatok elkerülése érdekében.
A kockázat menedzsmenteket helyesen alkalmazó szervezetek kevesebb incidensre számíthatnak. Egy átfogó szemléletmód kialakítása szoros összefüggésben, és egyenes arányosságban van a hatékonysággal és az incidensek számával.

Az informatikai technológia ilyen kiemelt szerepe komoly veszélyeket is rejt magában. Minél bonyolultabb egy adatkezelő rendszer, annál nagyobb fenyegetettségnek van kitéve, a működésük során fellépő hibák pedig rendkívül súlyos veszteségekkel járhatnak.

A fenyegetések, veszteségek kialakulásának megelőzésére, megakadályozására hivatott az IT kockázat menedzsment, amely önálló területté nőtte ki magát. Feladata, hogy a rendszert fenyegető veszélyeket felmérje, a megfelelő védelmi stratégiát kidolgozza. Csak komplex, átfogó, mindenre kiterjedő stratégiák alkalmazása segítségével küszöbölhetők ki a gyenge pontok által bekövetkezhető

[21] Információbiztonsági helyzetkép 2011.

fenyegetések. Olyan szilárd rendszer kialakítására kell törekedni, amely minden pontján egyenlően erős, ezáltal hatékonyvédelmet képes nyújtani.

Az informatikai rendszerek biztonságának megteremtése magában foglalja a következőket:

- számítástechnikai eszközöket, rendszereket,
- informatikai rendszerek környezetét,
- informatikai rendszerekkel kapcsolatba kerülő személyeket,
- a rendszerekre, üzemeltetésükre vonatkozó szabályozásokat, előírásokat, dokumentumokat

Az informatikai rendszerek védelmét jelentősen befolyásolja, hogy ahány szervezet, annyiféle kockázati profil létezik, azonban vannak olyan általános szabályok, amelyek figyelembe vétele, és a kockázatmenedzsmentbe való beépítése igen fontos. Ezek a következők:

- **nincs tökéletes biztonság;**
- a helyes kockázatelemzés feltétele, hogy tisztában legyünk azzal, hogy milyen elemekből áll az adatkezelő rendszer, milyen helyzetben üzemel, ki és hogyan üzemelteti;
- belátáson alapuló biztonság helyett „biztonságtudatos magatartást” tartsunk szem előtt;
- egységesítésre való törekvés – **szabványosítás**
- saját információs vagyon értékének ismerete
- a szervezet saját biztonságával kapcsolatos szándéka (betartás, betartatás);
- általános és helyi szabályzók összehangolása;
- fel kell ismerni, hogy a kockázati tényezők milyen súlyúak az adott rendszer esetében, meg kell becsülni bekövetkezési valószínűségüket;
- alapelvek érvényesülése;
- hatékonyság, objektivitás;
- **a dokumentálás pontos, jól érthető, folyamatos legyen**

A kockázatelemzés legfontosabb előnyei az alábbiak:

- a potenciális veszélyeket módszeresen azonosítja;
- kiszűri a „gyenge láncszemet” ez azért fontos, mert minden rendszer olyan erős, mint a benne lévő leggyengébb láncszem;
- kockázati rangsort állít fel;
- mélyen képes megismerni a rendszer szerkezetét;

- lehetséges módosításokat, megoldásokat ajánl a kockázat csökkentése érdekében; (feltárja a legjobb, leghatékonyabb technológiákat)

A kockázatelemzés során és az informatikai adatkezelő rendszer teljes működése során működni kell a következő alapelveknek:
Bizalmasság elve: az információ csak annak a személynek számára legyen elérhető, aki erre fel van jogosítva, mindenki más részére elérhetetlen legyen.
Sértetlenség elve: biztosítja az adat változatlanságát, a rendszernek jelezni kell, ha a benne lévő információt megváltoztatták (beszúrás, törlés, helyettesítés)
Rendelkezésre állás elve: akinek szükséges hozzáférni az adathoz, az a személy bármikor el tudja érni, ugyanis emberéletek, anyagi javak nagymértékű biztonsága függhet ettől.

A kockázatmenedzsment folyamata tudatos tevékenységsorozat, mely kockázatértő szemléletre, elemzési és kockázatkezelési módszerekre, eszközökre épül. Fontos, hogy ezt a folyamatot szabályozzuk, felügyeljük és kontrolláljuk. Ehhez elengedhetetlenül szükséges egy elemző, jól felkészült munkacsoport, melyet az adott szervezet tagjaiból is választhat a szervezet vezetője. Amennyiben a szervezet nem rendelkezik ilyen munkatársakkal, úgy külső szakértők segítségét is igénybe lehet venni. Nagyon fontos, hogy a szakértő képzettségi szintjét is dokumentáljuk, mint bármi mást ebben a folyamatban.[22]

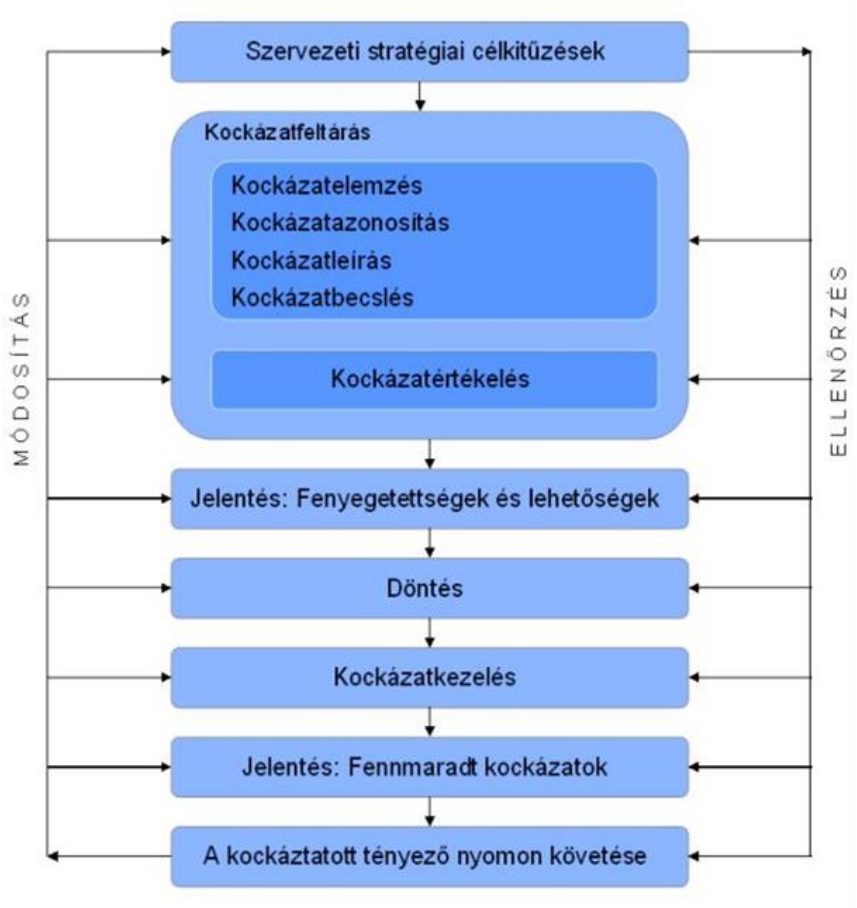
4. A Kockázatmenedzsment folyamataA[23]

Célszerű a működési tevékenységből származó kockázatok felismerését tudatosan, folyamatszerűen kezelni, ugyanis a fel nem ismert és nem kezelt kockázatok hatásaira, költségeire kevésbé gondolnak a döntéshelyzetben lévő vezetők, pedig azok jóval magasabb összeget és károkat eredményezhetnek, mint a kockázatelemzésbe fektetett pénz.

A kockázatelemzés kizárólag korszerű módszerek, eszközök, technikák esetén valósítható meg, amely egy szervezeti egységben végzett csapatmunka. Célja az emberi sérülések, és anyagi javak sérülésének megelőzése, környezeti hatások

[22] Dr. Rajnai Zoltán-Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, (AARMS - ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE) 9: (1) pp. 15-23. ZMNE, 2010
[23] Kockázatelemző módszrek és eszközök (Management Control and Compliance Control) Véry Zoltán 2008.

szabályozása, megelőzése, csökkentése, az elviselhető kockázat mennyiségének és mértékének meghatározása. Mivel az IT rendszerek kiemelten fontossá váltak az elmúlt évtizedekben, fokozódik a tőlük való függőség, ennek következtében az IT kockázat fő veszélyforrássá vált a szervezetek számára.



A fenti ábra mutatja, hogy a kockázatmenedzsment első lépése, hogy a szervezet fogalmazza meg célkitűzéseit, stratégiáját. Tárja fel azokat a tényezőket, melyek potenciális veszélyt jelentenek. Ez azért nehéz feladat, mert a károk általában nem közvetlenül fejtik ki hatásukat, hanem a velük kapcsolatban lévő rendszerelemeken keresztül az egész szervezet működésére hatással lehetnek. Például egy adatkezelő rendszerben javítást és cserét hajtanak végre, ennek hatására információvesztés, kiesés léphet fel, ami nagy kockázatot jelenthet. Következménye lehet ennek, hogy az üzleti folyamatok szintje , vagy a szervezet népszerűsége csökken, illetve ezáltal bevételkiesés is előadódhat.

Különböző kárkategóriák jelentkezhetnek, melyeket három csoportba oszthatunk:

- elsődleges kár (tényleges helyreállítás költsége, javítás, adatok pótlása)
- másodlagos kár
- harmadlagos kár (akár a szervezet teljes vesztesége)

A kockázatelemzés célja olyan megoldást találni, amely a teljes rendszer védelmét lefedi, minden elviselhető mértékű kockázatot legalább elviselhető mértékűvé csökkent, vagy megszüntet. Lehetőség szerint mindez költség hatékony is legyen! A kockázatmenedzsment egyik legfontosabb lépcsőfoka a kockázatok kezelése, melynek többféle módja lehet. A *veszélyforrások megszüntetésére* csak elméletben van lehetőség, hiszen nincsen teljes kockázatmentesség, mindig adódhat váratlan esemény. *A bekövetkező valószínűség és az okozott kár csökkentése* a gyakorlatban a legkedveltebb stratégia, a kettő kombinációja jelent optimális megoldást a kockázat kezelésére. *A kockázatok áthárítása* azt jelenti, hogy a veszély bekövetkezte előtt, már a szerződéskötés során átruházzuk a partnerre a terhek bizonyos részét. Jó példa erre az interneten történő vásárlás, amikor az e-boltok weblapjai nagyon körültekintők a vásárlók bankkártya adatait illetően, de ha adatlopás történik, azért nem vállalnak felelősséget, tehát áthárítják a kockázatot. Egy másik lehetőség a kockázatok kezelésére a *biztosítás.* Ez általában nem kifizetődő, ugyanis a biztosítási összeg általában nagyobb, mint az okozott kár mértéke lehet. A kockázatkezelés egy másik módja a *tudatos kockázatvállalás*. Amikor a védekezésre fordítandó összeg olyan nagy, annyira meghaladja a maximális veszteség mértékét, megéri tudatosan felvállalni a kockázatot. Ebben az esetben viszont tisztában kell lenni a következményekkel, vagyis a lehetséges veszteség másodlagos, harmadlagos mechanizmusával.

5. Magyarországi helyzetkép az IT biztonság képesség terén

2011-es adatok szerint Magyarországon átfogó biztonsági stratégia a szervezetek 61%-ánál van jelen, vagyis 4%-kal elmaradunk a nemzetközi átlagtól. Meg kell jegyezni, hogy ez az arány általánosságban magasabb a pénzintézetek esetében hazai és nemzetközi szinten egyaránt. Lényeges adat az is, hogy míg í 100%-ban magyar tulajdonú szervezetek 59%-a rendelkezik átfogó biztonsági stratégiával, addig ez az arány 82% a nemzetközi – magyar tulajdonú szervezetek esetében. A 2011-es helyzetkép[24] alapján elmondható, hogy a szervezetek vezetői 75%-ban jól informáltak az általuk vezetett cég incidenseiről (például eszközlopás, külső behatolási kísérlet, stb.), nemzetközileg a vezetők 67%-ával szemben. A felelősség,

[24] Információbiztonsági helyzetkép 2011.

beszámoltatás terén komoly elmaradásunk van, ugyanis a szervezetek mintegy felénél nincs kinevezett informatikai biztonsági felelős. Ezen a téren is erős a pénzügyi szektor, a magánszféra is erősebb az átlagnál. Elemzők szerint a hiányosságok a gazdasági válságot nagymértékben okolják azért, hogy a vezetők „szemet hunynak" az IT biztonság támogatása felett. Az azonban ki kell hangsúlyozni, hogy 2010 óta a szervezetek tudatossága nőtt, emelkedtek a kockázatelemzésre fordított kiadások, szigorodtak az állami szabályozások. Minél nagyobb egy szervezet, annál inkább ki van szolgáltatva a biztonsági kockázatoknak, ugyanakkor a pénzügyi és a távközlési szektor a leginkább kockázattudatos. Kockázatelemzési programmal 2011-ben a szervezetek negyede rendelkezik, rendszeres mély IT kockázatfelmérést 40% végez, míg 34% tervezi ezt.

6. Kockázatelemzési módszerek

Kockázatmenedzsmenttel foglalkozó szakemberek számos módszert dolgoztak ki a kockázatelemzés korszerűsítése, szakszerűsítése érdekében. Feltehetjük a kérdést, hogy melyik a legjobb, leghatékonyabb ezek közül? Erre a kérdésre nagyon nehéz válaszolni, mert hogy nincs száz százalékos kockázatmentesség, úgy nem jelenthetjük ki egyik módszerről sem hogy a legjobb, hiszen a különféle szervezetek profilja más és más. Az a módszer, ami kiváló a banki szférában, nem biztos, hogy például a védelmi szférában is ugyanolyan hasznos. Vannak azonban olyan szempontok , amelyek figyelembevétele igen hasznos a kockázatelemzési módszer kiválasztásakor.

Ezek a következők:

- Olyan módszert válasszunk, amely az adott adatkezelő rendszerre jól alkalmazható, legyen tudományosan igazolható. A módszer kiválasztásakor figyelembe kell venni az adatkezelő rendszer életútját, kidolgozottságának fázisát. (Egy kialakítandó rendszer esetében nem szükséges részletes módszerek alkalmazása, ellenben egy bonyolult, sok adatot feldolgozó rendszer esetén a módszerek részletezhetők, finomíthatók).
- Sok esetben az „egyszerűbb több" – a helyesen alkalmazott egyszerű módszer hasznosabb eredményt hozhat, mint a bonyolultabb, kifinomultabb, de rosszul elvégzett elemzés.

Fontos megjegyezni a nyomon követhetőséget, mellyel az egész elemzést igazolni tudjuk. Ennek egyik fontos része a dokumentáltság. Az elemzés minden egyes

fázisát jól érthetően, világosan kell megadni a félreértések, pontatlanságok elkerülése miatt.
A kockázatelemzési módszerek, ajánlások széles választékából néhány ismert módszert érintőlegesen említek meg, három népszerű módszertant részletesebben jellemzek és vetek össze.

Fuzzy logika
A Fuzzy logika alapú kockázatbecslés lényege, hogy egy időben több logikai szabályt, szabálybázist alkalmaz, melyek kiépítését fogalmak és kategóriák definiálásával kell kezdeni. Ez a módszer gynevezett Kockázat becslési mátrixot alkalmaz.

Monte Carlo szimuláció
Ez egy valószínűség elemzési technika. Ebben a módszerben nagy szerepe van a megérzésnek.

Marion eljárás
Ez egy négy szakaszból álló módszer, melynek előnye, hogy a vizsgált terület biztonsági állapotát nagyon szemléletesen ábrázolja. Európa szerte elterjedt eljárás, az EU-ban is használják.

Courtney eljárás
Ezt a módszert az 1970-es években fejlesztette ki az IBM Amerikában, Európába az 1980-as években kezdett népszerűvé válni.

CRAMM MÓDSZER
A CRAMM[25] módszert az Egyesült Királyság kormányának Központi Számítógépes és Telekommunikációs Ügynöksége (CCTA) [26] alkotta meg 1987-ben. Ezt a kockázatelemzési és menedzselési módszert több esetben frissítették, fejlesztették. A módszertan igen nagy előnye, hogy a feladatokat következetesen, fokról-fokra írja le, elkészül a kockázatok felmérése, elemzése, majd meghatározza a kockázatkezelést biztosító intézkedéseket. Ezeket az intézkedéseket az úgynevezett Informatikai Biztonsági Koncepció tartalmazza. A CRAMM módszer alkalmas arra, hogy informatikai kockázatok felmérésre, dokumentálásra kerüljenek, a kockázatokat csökkentő intézkedések kiválasztásra kerüljenek, a fennmaradó

[25] Risk Analysis and Management Method
[26] CCTA Central Computer and Telecommunications Agency

kockázatokat egyértelműen meghatározza. Ez a módszer egy, a gyakorlatban kivitelezhető eljárás, amely nem fogalmaz meg elvárást arra nézve, hogy egy szervezet szempontjából milyen kockázat fogadható el, tehát nem normatíva, hanem egy gyakorlatban kivitelezhető eljárás. A módszer alkalmazását elősegíti, hogy informatikai rendszerrel is támogatható, például vannak a CRAMM módszertan kivitelezését elősegítő szakértői rendszerek, melyek előre beépített adatbázissal felgyorsíthatják a kockázatelemzés elkészítésének folyamatát.

A CRAMM MODELL FELÉPÍTÉSE

A megalkotók 4 szakaszra osztották fel a módszertant.

1. szakasz a védelmi igény feltárása, amely két részből áll:

- *Felmérik* az objektumokat, informatikai alkalmazásokat és a feldolgozandó adatokat, melyeket védeni szándékoznak;
- *Értékelik* az informatikai alkalmazásokat és a feldolgozandó adatokat;

2 szakasz: fenyegetettségek elemzésének szakaszában feltárják azokat a fenyegető tényezőket, amelyek az 1. szakasz adataira, alkalmazásaira veszélyesek lehetnek.

- A fenyegetett rendszerelemek felmérése;
- Az alapfenyegetettség meghatározása;
- A fenyegető tényezők meghatározása;

3. szakasz: Ebben a szakaszban vizsgálják a fenyegető tényezők *hatását* az informatikai rendszerre, meghatározzák a lehetséges károk bekövetkeztének gyakoriságát és kárértékét.

- értékelik a fenyegetett rendszerelemeket;
- meghatározzák a károk gyakoriságát;
- Meghatározzák a kockázatokat (kockázat = kárérték és bekövetkezési gyakoriság szorzata)

4. szakasz: Ez a feltárt kockázatok kezelésének szakasza.

- Kiválasztják a megfelelő intézkedéseket;
- Értékelik az intézkedéseket a bekövetkezhető károk csökkentése érdekében;
- Elemzik a költség és haszon arányát;
- Végül elemzik a maradvány kockázatokat.

Ebben a szakaszban döntenek arról, hogy elfogadják a maradvány kockázatot, vagy csökkentik.

A négy szakaszos kockázat felmérés és kezelés után készítenek el egy biztonsági koncepciót, melyben a következők kerülnek rögzítésre:

1. A biztonsági stratégia: célok, alapelvek, felelősségi határok.
2. A jelenlegi állapot rögzítése a kockázatelemzés eredményei alapján.

3. Az intézkedések kiválasztása, meghatározása.
4. Az intézkedések kölcsönhatásainak felmérése.
5. Az intézkedések szervezet működésére gyakorolt hatása.
6. Az intézkedések elfogadhatósága a költség – haszon arány figyelembe vételével.
7. A kockázatok állapotának megítélése, a maradvány kockázatok mértékének tudatosítása.
8. A maradvány kockázatok elviselhetőségének elemzése.

Korábban már említettem, hogy a CRAMM módszert folyamatosan frissítették, fejlesztették. Az előző 4 szakaszos változat mellett érdemes tanulmányozni az úgynevezett 5. változatot, amely három szinten elemzi a kockázatokat, de mindegyik szint átfogó kérdéssorral és útmutatóval rendelkezik.

Az 5. változat modellje:

1. szint

Első lépésben megállapítják a biztonsági szempontokat, meghatározzák a kockázat elemzés/kezelés elemeit. Azonosításra és értékelésre kerülnek a rendszer vagyonelemei is. Azonosítás után feltárják az üzleti hatásokat, melyek sértik a vagyonelem rendelkezésre állását, bizalmasságát és sértetlenségét.

2. szint

Ezen a szinten valósul meg a kockázat értékelése a biztonsági követelmények alapján. Megállapítják a fenyegetések fokát és típusát, amelyek megfelelő védelem nélkül potenciális veszélyt jelentenek a rendszer működésére.

Meghatározzák azokat a sérülékenységeket is, amelyeken át a fenyegetés megvalósulhat.

Végül összevetik a fenyegetések és sérülékenységek halmazát, majd ezekből megbecsülik a kockázati értékeket.

3. szint

Az utolsó lépésben meghozzák azokat az ellenintézkedéseket, melyekkel megfelelő védekezést lehet nyújtani a 2. szinten leírtak szerint. Nagyon fontos, hogy az ellenintézkedések mértéke kockázatarányos legyen.

A módszer gyakorlati megvalósulásának lépései:

1. Vagyonleltár készítése (vagyontárgy azonosítása, értékelése)
2. Sebezhetőség vizsgálat
3. A lehetséges fenyegető tényezők összegyűjtése
4. Támadható felületek (sebezhetőségek) azonosítása
5. Kockázatértékelés: a sikeres támadás valószínűségének és a vagyontárgyakban okozott kár mértékének becslése.

6. Védelmi intézkedések meghozatala, bevezetése
7. Védelmi intézkedések működtetése, ellenőrzése
8. Kockázatok újraértékelése

7. A COBIT nyíilt szabvány

Az informatikairányítás világszerte egyre szélesebb körben elismert eszköze, egyben nyílt szabványa a COBIT (CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY), amely rendszerbe foglalja az információ, az információ technológia és az ezzel kapcsolatos kockázatok kontrollálására alkalmas gyakorlatot. Hasznosítja az informatikairányítás korábbi eredményeit, ugyanakkor épít a korszerű vállalatirányítási módszerekre is. Hangsúlyozza, hogy az informatikának az üzleti célkitűzéseket kell szolgálnia. A COBIT alkalmazásával az üzleti területi vezetők, a működési kockázatokkal foglalkozó szakemberek, az informatikusok és az auditorok egységes szemléletben, közös fogalmi rendszert használva, hatékonyan tudnak együttműködni. Ezek az ismérvek a COBIT-ot kifejezetten érdemessé teszik a pénzügyi intézményekben való alkalmazásra. A pénzügyi intézmény informatikai rendszerének védelmére vonatkozó törvényi előírások és a COBIT megfeleltetését az I. sz. melléklet tartalmazza. A megfeleltetés a két anyag között természetesen – keletkezésük, készítőik, céljuk, felhasználási körük stb. különbözősége miatt nem lehet teljesen egyértelmű és megfellebbezhetetlen, de célja mindenképpen a jogszabálynak a nemzetközi gyakorlat alapján kialakított és karbantartott COBIT szabványhoz való igazítása és annak teljes lefedése. A nem egyértelmű megfeleltetés következtében tehát a COBIT bizonyos fejezetei több jogszabályi pontnál is megjelennek.

8. Történeti áttekintés, általános jellemzés

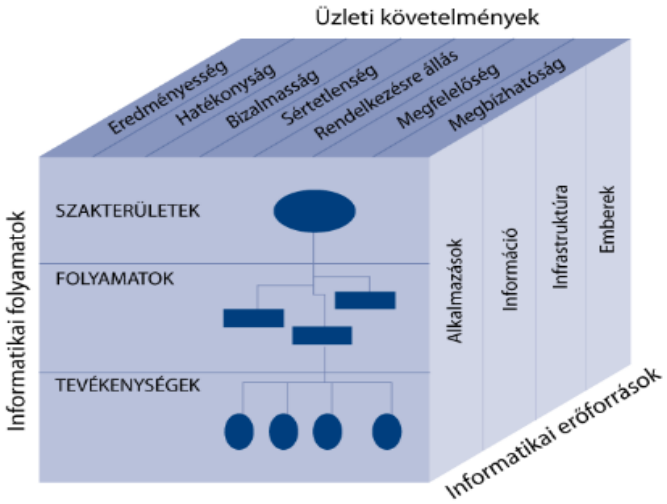
A szabványban megtestesülő kutatások motorja a világszerte kb. 35000 tagot számláló ISACA (Information Systems Audit and Control Association), amelynek társintézménye, a COBIT-ot kiadó IT Governance Institute (USA) 1998-ban alakult. Eddig három COBIT kiadás jelent meg: 1996-ban, 1998-ban és 2000-ben. 2003-ban megjelent egy internetes változata, továbbá egy egyszerűsített, bevezető verzió is. 2005-ben bevezetésre került a COBIT 4, de 2007-ben megtörtént ennek felülvizsgálata, mely COBIT 4.1 néven vált ismertté. A módszertan legfrissebb változata COBIT 5. néven 2012. júniusában jelent meg, melyhez kiadtak egy dokumentumot 2013. júniusában. A COBIT növekvő nemzetközi elfogadottságához jelentősen hozzájárul részletesen kidolgozott auditálási módszertana is. A

Felügyelet informatikai ellenőrei az ISACA tagjai és már több éve COBIT szemléletben végzik a pénzügyi szervezetek informatikai rendszerének vizsgálatát, és erre épül a jelenleg használt vizsgálati módszertanuk is.

A COBIT célja nemzetközileg és általánosan elismert kontroll célkitűzések vizsgálata, fejlesztése, kiterjesztése, melyek jól használhatók biztonsági szakértők számára.

Az alábbi ábrán található COBIT kocka tetején látható „Üzleti követelmények" dimenziója tartalmazza azokat az alapelveket, amelyeket az eredmények elérése érdekében alkalmaznak az eljárás során.

- Minőségi követelmények
    1. eredményesség (az üzleti igényeknek feleljen meg)
    2. hatékonyság
- Biztonsági követelmények
    3. bizalmasság
    4. integritás (teljesség)
    5. rendelkezésre állás
- Bizalmi követelmények
    6. megfelelőség (az elvárásoknak feleljen meg)
    7. megbízhatóság



Az ábrán a COBIT kocka látható, amely 3 dimenziós egységet alkot. A COBIT az ellenőrizendő informatikai tevékenységekben 4 területe különböztet meg:

1. Tervezés és szervezet (PO) (az informatikai stratégia megalkotása, szervezési kérdések)
2. Beszerzés és megvalósítás (AI)
3. Szolgáltatás, támogatás (DS)
4. Felügyelet (M) (az informatikai folyamatok felügyelete, vizsgálata, értékelése)

A COBIT kialakítása és fejlesztése a kezdeti szakasztól az egyszerűsödés irányába halad.

9. COBIT 5.

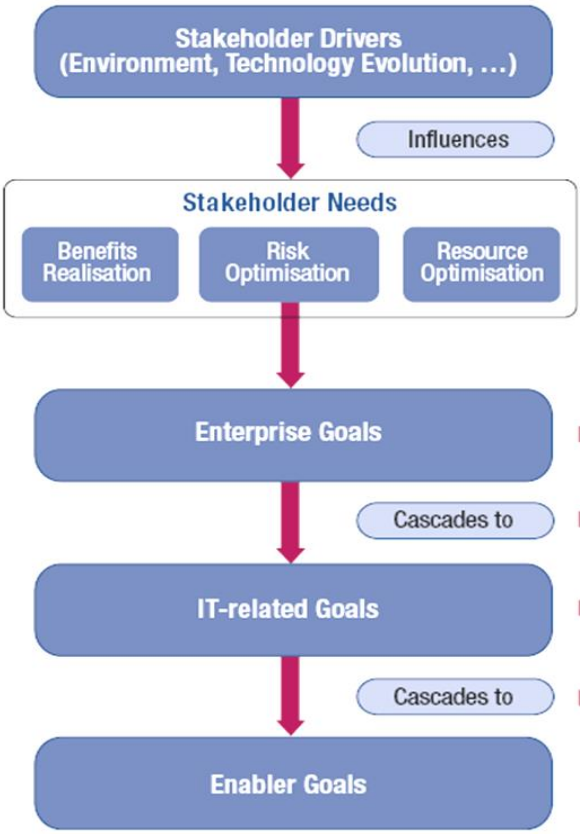
Ez az ISACA által kidolgozott kézikönyv az egyik legjelentősebb nemzetközi nyílt szabvány, amely alapján az IT rendszerek menedzselését, üzemeltetését, fejlesztését, biztonságosabbá tételét és ellenőrzését meg lehet valósítani. A COBIT 5. az IT irányítási menedzselési és auditálási keretrendszert összekovácsolja az ISACA többi kézikönyvével (BMIS[27], ITAF-IT[28], Risk IT-IT RMF[29], ValIT[30]).
A COBIT 5 tehát a COBIT előző verzióira épül, továbbfejlesztve azokat. Azok a felhasználók, akik ismerik a COBIT 4.1 verzióját, könnyen át tudnak lépni a COBIT 5-re, élvezhetik ennek a fejlett útmutatónak az előnyeit. A COBIT 5 az alkalmazói számára több lényeges terület esetében ad iránymutatást. Természetesen központi elemként kezeli a szabályozást, de nagy hangsúlyt helyez a folyamatokra, a szervezeti struktúrára és a szervezeti kultúrára is. Emellett kiemelten foglalkozik a különféle erőforrásokkal, amelyekbe beletartoznak az információk, a szolgáltatások, az infrastruktúrák, a különféle alkalmazások valamint maguk az emberek is. A COBIT 5 az emberek képességeinek, kompetenciájának kérdéskörét is kiemeli, ami a mindennapi döntéshozatal sikerét valamint az üzleti tevékenységek elvégzését jelentősen befolyásolhatja. Az új COBIT kidolgozásakor fontos szempont volt az is, hogy a különféle szabványokkal való integráció, együttélés az eddigieknél könnyebben valósulhasson meg.
A COBIT 5 alkalmazása során központi szerepet kap az **értékteremtés** és az **üzleti cél**.

[27] Business Model for Information Security
[28] IT Assurance Framework
[29] Risk IT-IT Risk Management Framework
[30] Value of IT

Értéket teremteni azt jelenti, hogy hasznot termelni egy optimális forrásköltséggel, optimalizált környezetben. Az üzleti cél maga az értékteremtés, amely az érintettek szükségleteit is képviseli.
E két fontos összetevő megteremtésekor fontos azt az alapelvet figyelembe venni, hogy az érdekeltek igényei találkozzanak. A COBIT 5 ezeket az igényeket a következőképpen hangolja össze:

- figyelembe kell venni a környezet, technikai fejlődés hatásait.
- fontos szempont, hogy mik az érintettek szükségletei (haszon, megvalósítás, kockázat optimatizálás, forrás optimatizálás)
- összesíteni kell a vállalkozás eredményeit
- fontos a képesség eredmények felmérése
- T-vel összefüggő eredmények kimutatása

Ezeket az igényeket az alábbi ábra szemlélteti



Cobit 5 2012. ISACA

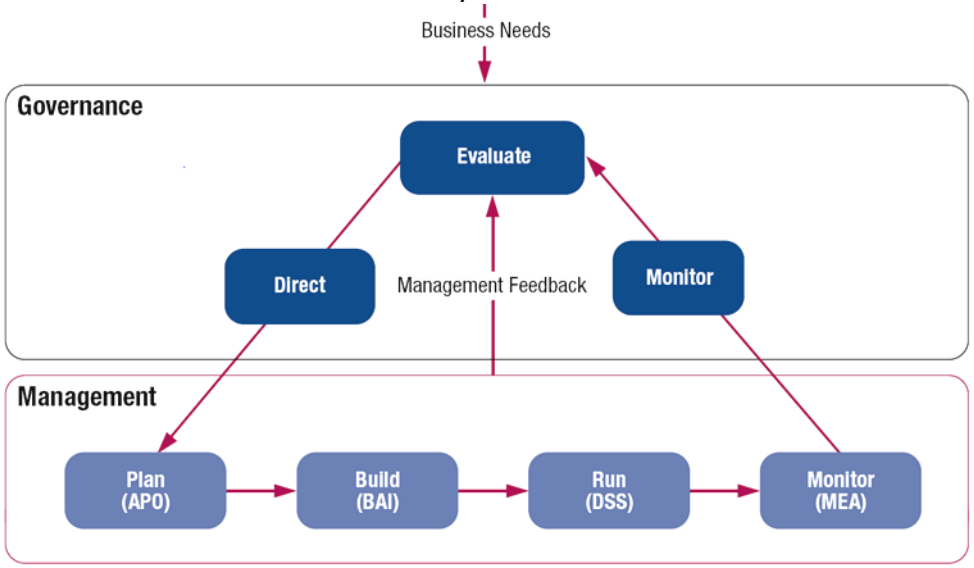
Irányítási és vezetési meghatározás

A COBIT 5 módszer két fő területre oszlik fel: vezetésre és irányításra. A vezetés és irányítás további részekre bontható

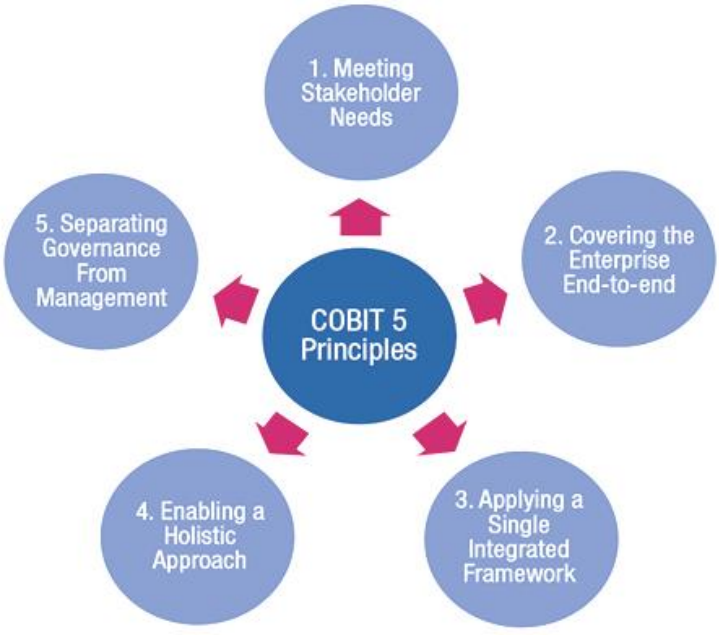
A vezetés területe feldolgoz, értékel, vezeti és felügyeli a meghatározott gyakorlatokat. Az irányítás összhangban van a tervezés, építés, futtatás és figyelemmel kísérés felelősségi területekkel, mint azt az alábbi ábra mutatja:

A COBIT 5 módszertannak öt alapelve van, amelyek alkalmazása a módszert sikeressé és igen jól alkalmazhatóvá teszik:

1. Találkozzon az érintettek igényeivel
2. Fedje le a vállalkozást az elejétől a végéig
3. Egyetlen integrált keretet alkalmazzon
4. Tegye lehetővé a holisztikus megközelítést
5. Különítse el a vezetést és az irányítást



Cobit 5 2012. ISACA



Cobit 5 2012. ISACA

10. A CRAMM módszer értékelése

Előnyei:

- A módszer átfogóan közelíti meg a kockázat elemzés és kezelés feladatkörét.
- Szoftverrel, és jól használható sablonnal támogatott.
- Intézkedések széles választékát ajánlja a kockázatok csökkentésére.
- Szükséghelyzetben is eszközt nyújt.
- Egy alapos biztonsági audit elvégzésére ösztönöz az informatikai rendszerben.
- Nagyon széles körben használt módszer (pl. NATO), ezáltal sok tapasztalati tényezőt beépítettek a módszerbe, ezáltal fejlődött, kikristályosodott a módszertan.
- Kockázatelemzése alapos, részletes, segítségével a kockázatok ól meghatározhatók.

Hátrányai:

- Ezzel a módszertannal hosszadalmas a kockázatelemzés, a kockázatok nem határozhatók meg egzaktul, költséges a hosszadalmas vizsgálat miatt.

- Hónapokat is igénybe vehet a rendszer elemzése, amely miatt az eredmények gyorsan túlhaladottakká válhatnak.
- A módszer kvalitatív jellege miatt nehezebb pontos értékeket meghatározni.

11. A COBIT módszertan értékelése

Előnyei:

- A Governance Institute az egész világot képviselő független szervezet, ezért lehetőség nyílik arra, hogy minden kontinensen, egyre szélesebb körben fogadják el a szabványt.
- A COBIT növekvő nemzetközi elfogadottságához jelentősen hozzájárul részletesen kidolgozott auditálási módszertana.
- A módszertan kipróbált, jól bejáratott, jó alapot biztosít a kockázat felmérésekhez.
- Összpontosítás az adottságokra.
- A COBIT 5 alkalmazásakor fontos tényező, hogy olyan adottságok és források is szerepet kapjanak, mint az:
    - elvek, rendelkezések és keretek
    - folyamatok
    - szervezeti felépítés
    - kultúra, etika és viselkedésmód
    - információ
    - szolgáltatások, infrastruktúra és alkalmazások
    - emberek, képességek és kompetenciák

Hátrányai:

- Jelentős kezdeti energia ráfordítást követel meg, ebben az értelemben nem felhasználóbarát, nem kezelhető könnyen.
- Mivel jelentős anyagi befektetést igényel a módszer alkalmazása, ezért általában a jelentős, és fejlett informatikával rendelkező vállalatok tudják használni.
- A COBIT elsősorban felsőszintű irányelveket tartalmaz, a technikai részletekre nem tér ki. Teljesen átfogó, de nem minden esetben kínál specifikus lehetőségeket.
- Kvalitatív módszer, nem tartalmaz számszerűsíthető eljárásokat.

Összegzés

Mindkét módszertan kiválóan használható a kockázatelemzés és kezelés területén. A CRAMM módszer és a COBIT esetében is elmondható, hogy részletes, átfogó, jól kidolgozott. Külön kiemelem azt, hogy mindkét módszertan esetében a megalkotók az első verziók hibáit, hiányosságait felmérve a hibákat kiküszöbölték, a hiányosságokat pótolták annak érdekében, hogy olyan magas szintű módszertanokat alkossanak meg. Ezek valóban lehetőséget adnak arra, hogy a napjaink információs társadalmát érő fenyegetésekkel szemben a szakma fel tudja venni a versenyt, ezáltal valóban a „0 kockázati szint" irányába tudjon haladni, és megközelíteni azt.

Felhasznált irodalom

- Schutzbach Mártonné Az informatikai rendszerek biztonságának kockázatelemzése a védelmi szférában (Doktori értekezés, ZMNE, Budapest, 2004
- Rető Dávid: Kockázatértékelési metrika az információtechnológia auditálásában (Doktori értekezés, Budapesti Corvinus Egyetem, 2006
- http://rm-inv.enisa.europa.eu/methods/m_cramm.html
letöltve: 2013. 12.02. European Union Agency for Network and Information Security
- Üzletmenet folytonosság menedzsment (BCM)
http://www.szintezis.hu/upload/bcm_uwe4-0_termekismerteto.pdf letöltve: 2013. 12.02.
- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT (http://www.isaca.org/COBIT/Pages/default.aspx) letöltve: 2013. 12.02.
- 10 STEPS TO DO IT YOURSELF CRAMM (http://archive.is/Lc9m1) letöltve: 2013. 12.02.
- Dr. Rajnai Zoltán-Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, (AARMS - ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE) 9: (1) pp. 15-23., 2010.

Szente András[31]: Veszélyes technológiák kockázatelemzése

Absztakt
A publikáció a veszélyes technológiák kockázatelemzését foglalja egybe.

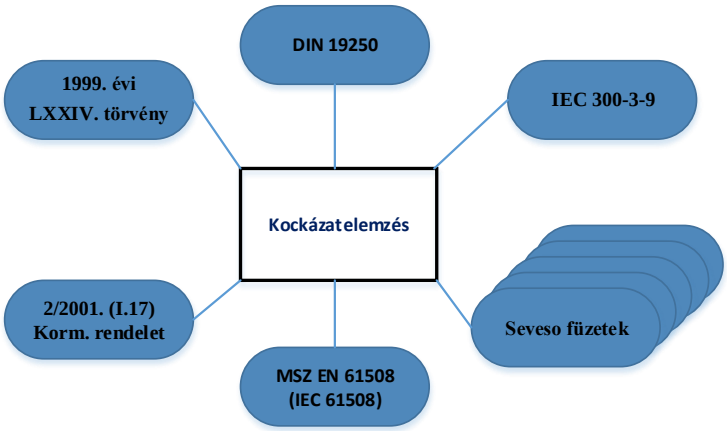
Abstract
This article shows risk management of dangeorus technologies

1. Jogszabályi környezet – kötelezettség a kockázat elemzésre

Magyarországon **1999. évi LXXIV. törvény** rendelkezik a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről, azon belül annak IV. fejezete kötelezi az üzemeltetőt kockázat alapú biztonsági jelentés és biztonsági elemzés készítésére. Ezen felül **a 2/2001. (I.17) Korm. rendelet** 3. sz. mellékletének 2.5 pontja rendelkezik a súlyos baleset által való veszélyeztetés „értékeléséről". Eszerint az üzemeltető az üzem által okozott kockázatot és a következmények értékelését együttesen figyelembe veendő módszert kell, hogy alkalmazzon. Az **IEC 300-3-9** (1995) a technológiai rendszerek kockázatelemzésére vonatkozó nemzetközi szabvány, melynek hazai kivonata megtalálható a Magyar Műszaki Biztonsági Hivatal Műszaki Biztonsági Főfelügyelete (MMBH/MBF) által kiadott Seveso füzetekben.
A **Seveso füzetek 1-5 kötet** (2001 – 2005) a veszélyes anyagokkal kapcsolatos súlyos baleseti veszélyek szabályozásával foglalkozik, az ún. „Seveso 2" irányelv szerint. A technológiai rendszerek kockázatelemzését a 3. füzet részletezi.
E szerint a kockázatelemzés három kérdésre keresi a választ:

- Mi romolhat el?
- Mennyire valószínű ennek a bekövetkezése?
- Melyek a következmények?

[31] Doktorandusz hallgató - Óbudai Egyetem Biztonságtudományi Doktori Iskola (szentea@freemail.hu)

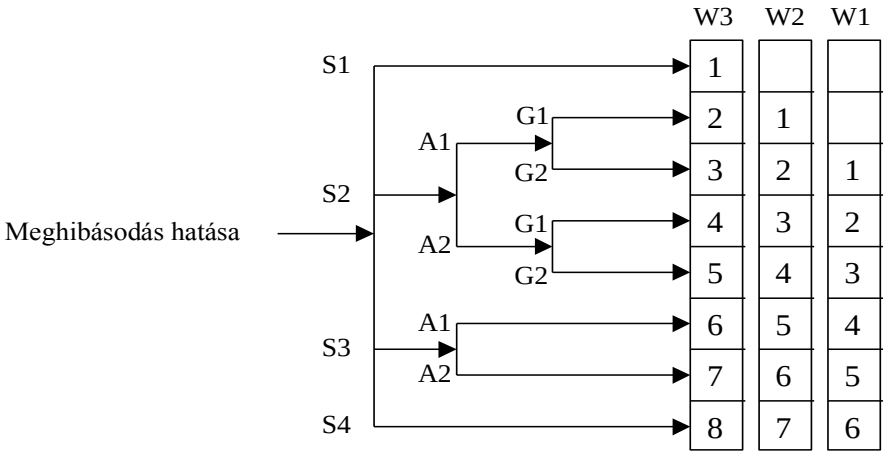


5. ábra

Az 1. ábra a kockázatelemzés hazai és nemzetközi jogi pilléreit szemlélteti. Meg kell jegyezni, hogy jelen anyag csak műszaki, valamint informatikai kockázat fajtákkal elemzési módszerivel foglakozik, ezen kockázat fajták sorolhatók egyértelműen a „technológiai kockázat" halmazába, a humán, pénzügyi, politikai, egészségügyi, természeti, stb., kockázat típusok értelemszerűen nem.

Kevésbé ismert és elterjedt a német **DIN 19250** szabvány, amely a „rizikógráf" használatát mutatja be. Veszélyes technológiák irányítórendszerinek kockázat alapú elemzésére hozták létre (2. ábra).

Nyolc biztonsági osztályba sorolja az irányítórendszereket, egyes a legalacsonyabb, nyolcas a legszigorúbb követelményeket jelenti. A szabvány négy kockázati paramétert tartalmaz: **S** (a veszélyesség nagysága), **A** (tartózkodási idő a veszélyes területen), **G** (veszélyelhárítás), **W** (a veszélyes esemény valószínűsége).



1. ábra

A kockázati paramétereken belüli felosztás:

S1: kisebb sérülés
S2: személy sérülése vagy egy személy halála
S3: több személy halála
S4: katasztrófa
A1: soha, nagyon ritkán
A2: gyakran, állandóan
G1: lehetséges
G2: nem lehetséges
W1: nagyon alacsony
W2: alacsony
W3: magas

Például az utasszállító rendszerek, forgalomirányító rendszerek hatos biztonsági osztályba tartoznak a szabvány szerint.

Az **MSZ EN61508 (IEC 61508)** nemzetközi és hazai általános biztonsági szabvány megdefiniálja a rendszerrel vagy berendezéssel szembeni követelményként megengedett veszélyességi gyakoriságot vagy valószínűséget (THR – Tolerable Hazard Rate). Az elvárt biztonság szintjének biztosításához egy másik biztonsági követelmény, a biztonságintegritási szint (Safety Integrity Level, SIL) fogalma is bevezetésre kerül, melyből négy tartomány létezik (SIL1-SIL4), ezek hozzá vannak rendelve egy THR tartományhoz. Idővel épültek a fenti alapszabványok köré továbbiak, illetve specializált tartalmat kaptak: DIN V 19251, biztonsági funkcióra használt mérő és vezérlő rendszerek biztonsági követelményei, IEC 61511, biztonság a folyamat iparban, DIN V VDE 0801, mikroprocesszorok biztonsági alkalmazásokban.
A kockázatbecslés folyamata a „Seveso füzetek” 3.sz. füzete alapján a 3. ábrán látható. Első lépés a rendszerelemzés alá vont rendszer meghatározása. Ezalatt a rendszer és környezetésnek általános bemutatása értendő, fel kell térképezni a rendszerhatárokon átmenő anyag, - energia, - és információáramlást. Definiálni kell az elemzés irányát meghatározó előfeltevéseket. A fentieket kockázatelemzési terv formájában dokumentáljuk. A veszélyelemzés és a következmények előzetes kiértékelésében a veszélyeket a veszélyek kialakulásának módjával együttesen szükséges azonosítani. Itt tehet az elemző helyesbítő intézkedéseket a veszély elkerülésére vagy csökkentésére. Ezen a ponton kell döntést hozni, hogy szükséges - e kockázatbecslés, vagy a kockázat mértéke olyan kicsi, hogy erre nincs szükség. A

folyamat központi elem a kockázatbecslés. Ennek során meg kell vizsgálni a releváns kezdeti eseményeket, körülményeket, eseménysorokat, valamint azok káros következményeinek valamennyi jellemző tulajdonságát, aspektusát. A kockázatbecslés során általában mennyiségi módszert alkalmazunk, amit célszerűen a vizsgált technológiának legmegfelelőbb módon kell megválasztani. Számszerűsége világítson rá a folyamat hiányosságaira, gyenge pontjaira. Egyik módja, a gyakoriság elemzés történhet irodalmi adatok alkalmazásával, analitikai vagy szimulációs eljárással, mérnöki értékítélet igénybe vételével. Ezeket a technikákat együttesen is lehet alkalmazni, ami esetenként határozottan előnyös lehet, ugyanis a diverz elemzési mód alaposabb értékítéletre nyújt lehetőséget. A következményelemzés a baleset bekövetkezése esetén a valószínű hatás becslése. Fontos, hogy a másodlagos, vagy dominóhatás által létrejött következményeket is monitorozzuk. A kockázat kiszámítása valószínűség számítás, statisztikai matematika, kockázateloszlás, eszközparkjával végezhető, ez ma számítástechnikával alátámasztott. A kockázatbecslés értelemszerűen bizonytalansággal terhelt, ahol lehet, azonosítani kell a bizonytalanság forrását, illetve az eredmény megadás tartalmazza a pontatlanság becsült mértékét. Értékítélet megfogalmazásakor a kedvezőtlenebb irányt, értéket kell alapul venni. Az elemzés igazoló ellenőrzése foglalja magába, hogy az elemzés összhangban van-e a kitűzött célokkal, igazolja, hogy megfelelő módszert, modellt, feldolgozási módot, adatokat használt. Az igazoló ellenőrzés elvégezhető az elemzés eredményének közvetlen megfigyelésen, szakértői véleményen alapuló összevetésével. A záró dokumentum, a kockázatelemzési jelentés jól érthetően foglalja össze a műszaki, technikai jellegű információkat, végeredményeket, konklúziót.

Az elemzés naprakésszé tétele a teljes életciklus alatt bármikor elvégezhető, új információ ismertté válása, üzemeltetési körülmény megváltozása, új igények felmerülése esetén kötelező.

2. Kockázatelemzési módszerek

Hibafa elemzés (FTA, Fault Tree Analysis)

A legáltalánosabban alkalmazott módszer a mérnöki rendszerek kockázat - és megbízhatóság elemzése területén. A módszert az **IEC 1025** (1990), **BS 5760-7** (1991) szabványok, hazai környezetben a **Seveso füzetek 4. sz**. füzete mutatja be. A hibafa egy olyan diagram, ami rendszeren belül kimutatja egy lehetséges kritikus esemény és az azt kiváltó okok közötti logikai kapcsolatot. Különösen jól

használható az űrhajózás, hadiipar, atomenergetika területén, ahol a minőség és biztonság elválaszthatatlan kritériumok. Deduktív módszer, melynek során hibás rendszer állapotot feltételezünk, amelyből kiindulva, visszafelé haladva határozzuk meg az okokat, vagyis, hogy a hibás rendszer állapot milyen okok kombinációjaként jöhet létre. A definiált eseményt, amiből kiindultunk, feltételezett kezdeti eseménynek, vagy csúcseseménynek nevezzük, míg az ok feltárás során keresett események az elemi események. A hibafák grafikus szerkesztése során közbenső események is generálódnak a végpontok között, melyek együttesen szemléletes, vizuális megjelenítést tesznek lehetővé, hierarchikus struktúrát alkotva. A hibafa szerkesztéséhez a logikai kapuk szimbólumrendszerét, vagy logikai függvényt használhatunk. Az események közötti logikai kapcsolatok az elektronikából, informatikából jól ismert kapcsolatok: ÉS, VAGY, NEM kapcsolat, illetve K/N típusú kapcsolat, ez utóbbi esetben N esemény közül legalább K számú bekövetkezése szükséges a kimenet bekövetkezéséhez. A módszer szemléltetéséhez nézzük azt a példát, amikor a kezdeti esemény egy gázszállító tartályautó tartalmának elvesztése (4. ábra). Látható, hogy ezt előidézheti a tartály anyag hibája, vagy tömlő - és visszacsapó szelep együttes hiba. Tömlőhiba szakadás vagy lyukadás útján állhat elő. A hibafa minőségi (kvalitatív) analízise során elvégezhetjük annak redukcióját, azaz a közbenső események feloldhatók, amennyiben diszjunktív normál alakra (VAGY logika) hozzuk a gráfot.

Meghatározható a minimális vágathalmaz, ami nem redukálható tovább, vagyis rámutat az üzemzavarhoz vezető leggyengébb útvonalra. Segítségével azonosítható a kritikus esemény, illetve az egyszeres hibapont (SPOF). A mennyiségi (kvantitatív) analízis során - az ábrán látható módon - az egyes eseményekhez hozzárendeljük azok valószínűségét. Ezekhez az adatokhoz gyártóművi adatként, becsléssel, vagy tapasztalati úton juthatunk.

Az eredő valószínűségeket a gráfon ÉS kapu esetén szorzat, VAGY kapcsolat esetén összegzés művelete adja, amennyiben az elemi események között nincs korreláció. Általános, i bemenetszámú ÉS kapu esetén az eredő valószínűség:

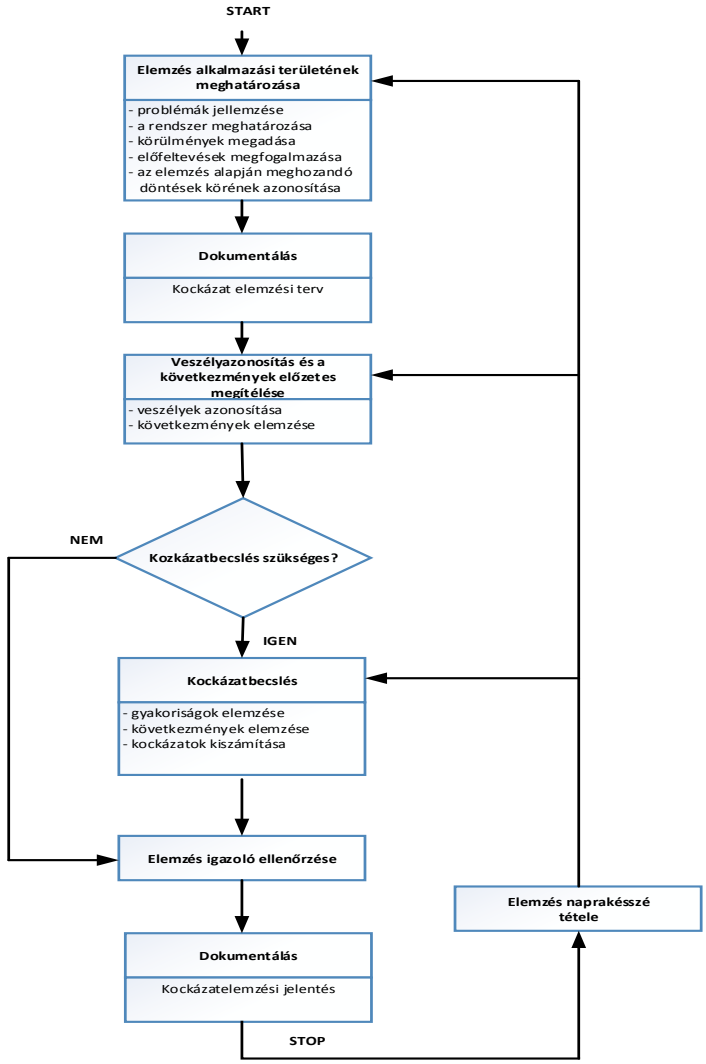
$$Q_{KI} = \prod_{i=1}^{n} Q_i$$

Általános, i bemenetszámú VAGY kapu esetén:

$$Q_{KI} = 1 - \prod_{i=1}^{n} [(1 - Q]_i)$$

Egybemenetű NEM kapu kimeneti valószínűsége:

$$Q_{KI} = 1\ Q_{BE}$$



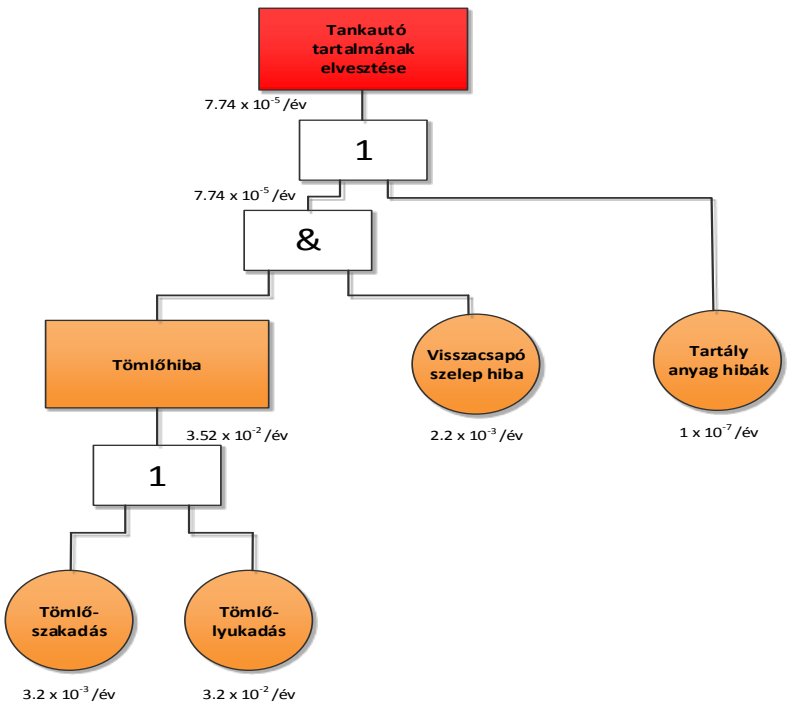
2. ábra

Látható, hogy a hibafa analízis gyenge pontjai az egymással keresztirányú összefüggésben lévő (korreláló) hibák, továbbá az időbeli hibák (szekvenciák)

kezelése. Jellegzetessége még a plauzibilitás, ami azt jelenti, hogy az egymás hatását kompenzáló, egyidejű belső hibákat nem veszi figyelembe. A hierarchikus felépítés, elemi kapukra történő bontás lehetősége az FTA módszer gyakorlati alkalmazhatóságát garantálja.

Az FTA módszert több modellező program használja, így az **Isograph** cég megbízhatóság elemző programcsomagja is, a Reliability Workbench V11.1.1. Vele történő számítógép alapú rendszer hiba modellezése látható az 5. ábrán. A rendszer hibát előidézheti alaplap hiba, vagy memória egység és kijelző hiba, vagy tápegység hiba. Meg kell jegyezni, hogy ezen szoftverek nem helyettesítik a vizsgált rendszer ismeretét, ugyanis a topológia kialakítása, input adatok bevitele az elemző feladata, amihez az adott technológia alapos ismerete elengedhetetlen.

A kockázati tényezők eredményeinek diagramba foglalása oly módon, hogy a balesetek különböző rendszerektől való függése átlátható, megérthető legyen. Mennyiségi kockázatelemzéshez használják. A hibafa elemzéssel ellentétben az eseményfa modell egy előremenő, induktív gondolkodású folyamat. Az elemzést a kiváltó esemény definiálásával kezdjük, ebből fejtjük ki az okozatként következő eseményláncokat, mint bináris eseménylánc logikát.



3. ábra

A 3. ábra egy két-redundáns komponenst tartalmazó rendszer melegtartalékolt - és hidegtartalékolt Markov modelljét szemlélteti.

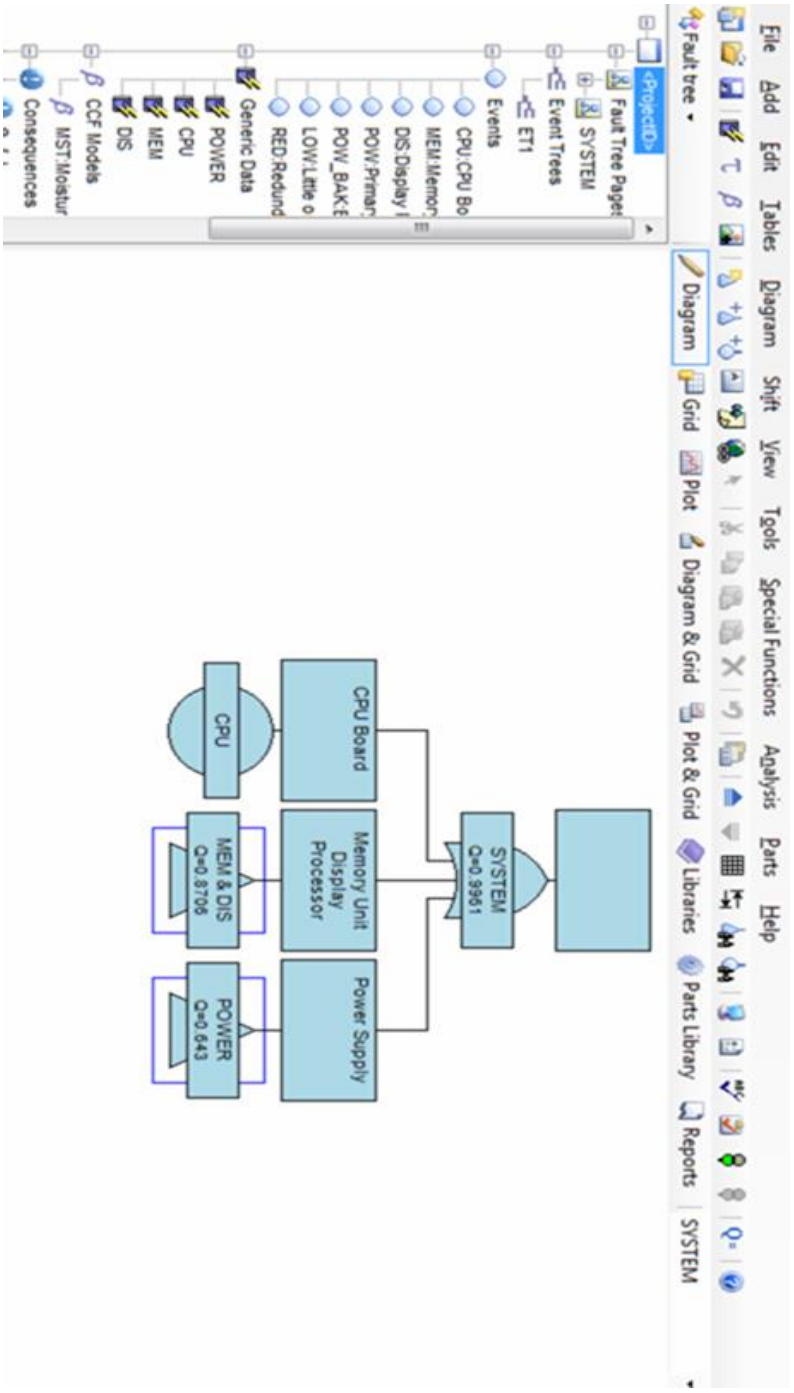
Állapotok: 1- Mindkét komponens üzemképes,
2- egy komponens üzemképes, egy üzemképtelen,
3- mindkét komponens üzemképtelen. λ a meghibásodási ráta, μ a javítási ráta.

A két tartalékolási módszer összehasonlítható az ábra segítségével.
Melegtartalékolt rendszer esetén, mivel mindkét komponens párhuzamosan, egy időben működik, a meghibásodási ráta kétszer akkora, mint hideg tartalékolt rendszer esetén. A rendszer eredő megbízhatósága **N** komponens esetén **N!** - szor nagyobb hidegtartalékolt rendszer esetén, mint meleg tartalékolás mellett.
Értelemszerűen nem mutatja (elfedi) az ábra a meleg tartalékolás automatikus és folytonos áttérésre vonatkozó előnyét, hiszen abban az esetben az garantált mindaddig, amíg van üzemképes komponens, míg hideg tartalékolás mellett a tartalék alkatrész üzembe vétele további külső körülmények (automatika, személyzet) függvénye. A szoftveres alkalmazás (9. ábra) egy öt állapotú rendszer Markov diagramját szemlélteti adott meghibásodási és javítási valószínűségekkel.
Jól alkalmazható a módszer társadalomtudomány kutatási, emberi erőforrás menedzselési problémák elemzése során is.

Eseményfa elemzés (ETA, Event Tree Analysis)

Általános lépései:

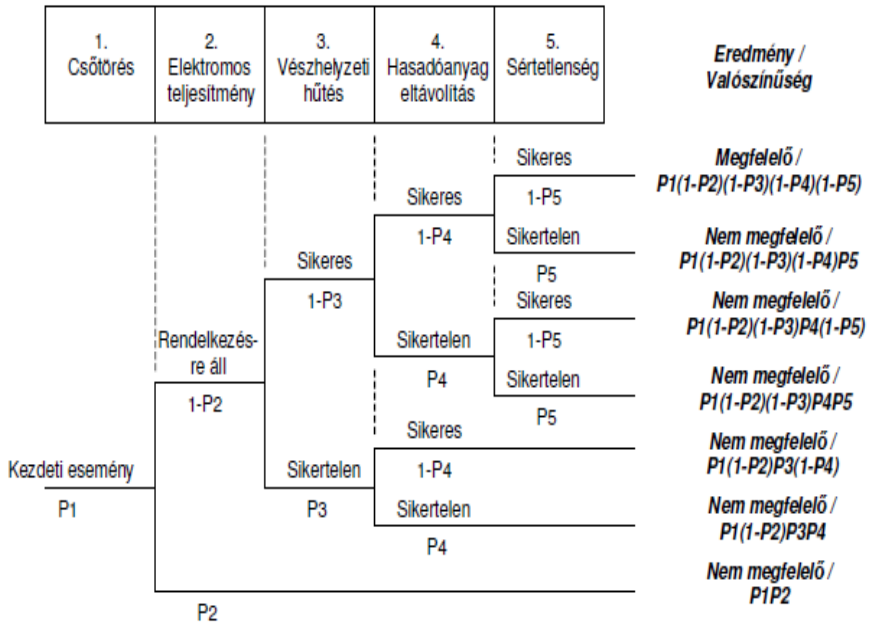
- kiváltó esemény kijelölése
- az eseményhez tartozó biztonsági funkciók definiálása
- eseményfa szerkesztése, időrendi sorrendben
- várható baleseti eseményláncok leírása


File Add Edit Tables Diagram Shift View Tools Special Functions Analysis Parts Help
Fault tree
Diagram Grid Plot Diagram & Grid Plot & Grid Libraries Parts Library Reports
SYSTEM
<ProjectDb
Fault Tree Page
SYSTEM
Event Trees
ET1
Events
CPU CPU Bo
MEM Memor
DIS Display
POW Prmar
POW_BAKE
LOW Little o
RED Redund
Generic Data
POWER
CPU
MEM
DIS
CCF Models
MST Moistur
Consequences
SYSTEM
Q=0.9951
CPU Board
Memory Unit
Display
Processor
Power Supply
CPU
MEM & DIS
Q=0.8706
POWER
Q=0.643

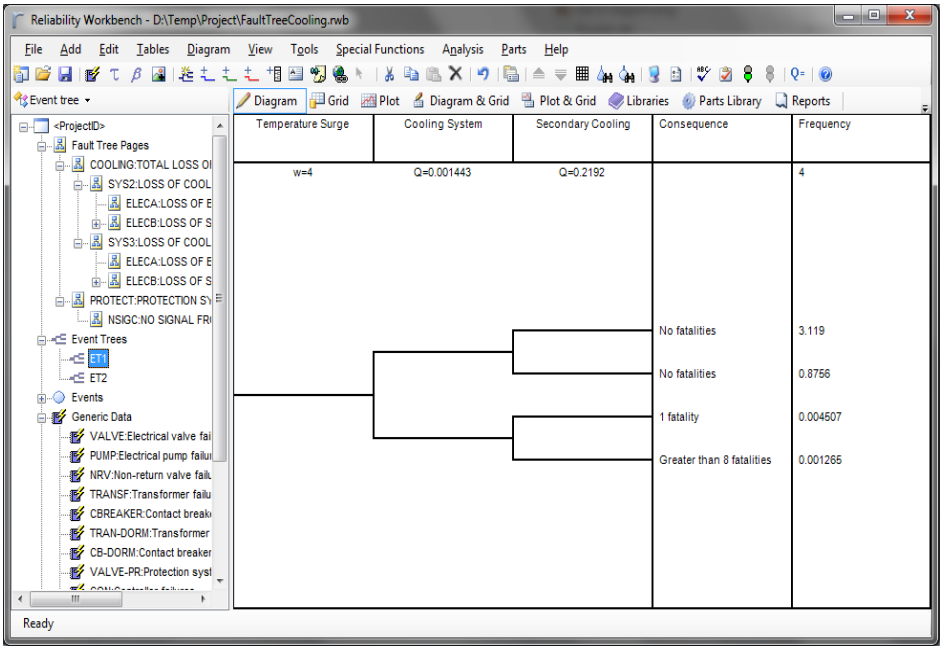
4. ábra

N darab esemény hatását vizsgálva az eseményfán $\mathbf{2^N}$ faág keletkezik, a különböző kétállapotú feltételek, meghibásodások bekövetkezésének, vagy be nem következésének a hatására. Az elágazásokat kiváltó eseményeket, amennyiben lehetséges időrendi sorrendben célszerű feltüntetni, így az eseményfa szekvenciát is tükröz. Ahol a sorrendiség nem megállapítható, vagy több egyidejű esemény létezik, nehézkes az alkalmazása. Az egyes ágak („vágatok") bekövetkezési valószínűsége a vágatot kialakító események bekövetkezési vagy be nem következési valószínűségeinek a szorzata, a soros elrendezés miatt. A gráf jobb oldalán az eredmény az alkalmazott algoritmussal együtt feltüntethető. Gyakran kombinálják az eseményfát a hibafával olyan módon, hogy az eseményfán az egyes elágazásokat kiváltó okok egy-egy hibafa csúcseseményei, így az egyenrangú események analízise is lehetővé válik. Az eseményfa modell egy példáját a 6. ábra szemlélteti, egy atomerőművi üzemzavar kialakulását elemezve [Leveson, 1995].

A Reliability Workbench V11.1.1. (Isograph) szoftverrel elvégzett eseményfa elemzés (7. ábra) egy rendszer hőmérsékleti tranziensének kialakulási valószínűségét szemlélteti, kétkörös hűtés mellett.



5. ábra



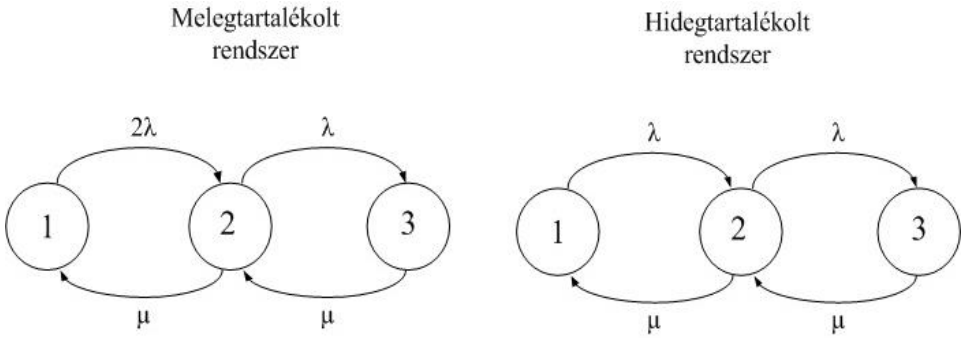
6. ábra

Markov analízis (Automata kockázati analízis)

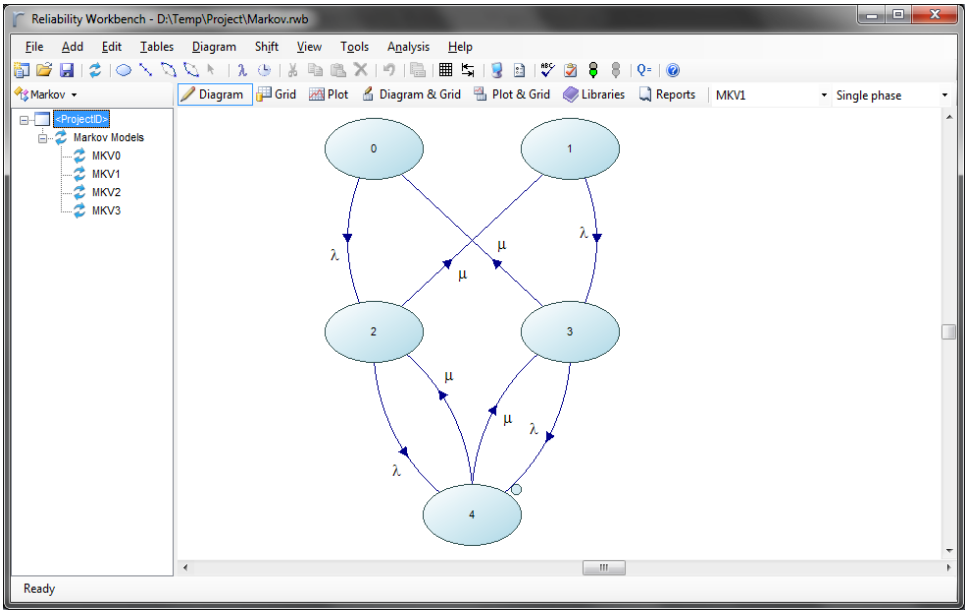
Állapot orientált elemzési módszer, az állapotgép (State Machine, SM) elméletet használja fel: amennyiben a rendszer az adott állapotban van, és az átmenet feltétele igaz, a rendszer az új állapotba kerül, végrehajtódik a kimenet. Az elemzés során fel kell térképezni a rendszer lehetséges állapotait, állapot átmeneteit, és ezek valószínűségét. Dinamikus viselkedés modellezésére alkalmas, viszont korlátot jelenthet a magas, átláthatatlan állapotszám.

Lépései:

- a rendszer állapotainak definiálása
- Vizsgált állapotok definiálása
- Állapotátmenetek meghatározása
- Állapotátmenetek gyakoriságának meghatározása
- Rendszer modellezés



7. ábra



8. ábra

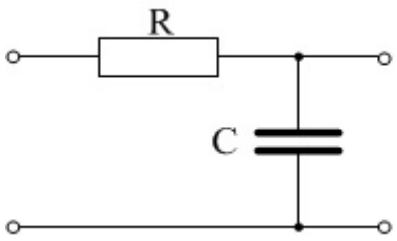
Hibamód - és hatás elemzés, valamint hibamód, hatás - és kritikusság elemzés (Failure Mode and Effect Analysis: FMEA, Failure Modes, Effects and Criticality Analysis: FMECA).

A módszer egy tetszőleges rendszer strukturált, minőségi (determinisztikus) analízise, melynek során feltárásra kerülnek a lehetséges rendszer meghibásodások és hatásuk (FMEA). Amennyiben kiegészül a hibahatás súlyosságának analízisével is, meghibásodási módok, hatásaik és kritikusság elemzésről beszélünk (FMECA). A módszert az **IEC 812** nemzetközi szabvány írja le.

Lépései:

- A vizsgálat alapjainak meghatározása
- Az analízis szintjének meghatározása
- Analizálandó egységek, alegységek meghatározása
- Valamennyi érintett komponens lehetséges meghibásodási módjainak összegyűjtése ("hibakatalógus")
- A hibakatalógusban definiált valamennyi hiba következményének feltárása
- A következmények osztályozása a rendszerre gyakorolt hatásuk alapján
- Az egyes meghibásodási módok detektálhatóságának a vizsgálata
- kompenzációs módok, változatok analízise a rendszerhibák minimalizálása céljából

Célszerű a vizsgálatot hierarchikusan végezni, lehet alulról felfelé („bottom-up”), bonyolult rendszerek esetén felülről kiindulva („up-bottom”). A strukturálás három módon történhet: strukturális modell alapján, vagyis a komponensek fizikai megjelenése, szeparáltsága alapján, funkcionális modell, vagyis a komponensek rendszerbeli feladata alapján, megbízhatósági blokkdiagram alapján, a redundancia meghatározásához soros-párhuzamos kapcsolatok segítségével. Az elemzés eredményét táblázat formájában rögzítik. A nagy fontosságú meghibásodásokra való rámutatáshoz a módszer kiegészül a kritikusság vizsgálattal (FMECA), automatizálási, elektronikai, autóipari területen használatos. Ehhez bevezetjük a kockázat prioritási szám (Risk Priority Number, RPN) fogalmát, mely három tényezővel határozható meg. Ezek a hiba fellépési gyakoriságának sorszáma, a következmény súlyosságának a sorszáma, a hiba detektálhatóságának a sorszáma. A három tényező szorzata adja a meghibásodás súlyára jellemző RPN számot, minél nagyobb ez az érték, annál kritikusabb az adott meghibásodás. A 10. ábra szerinti R - C aluláteresztő szűrő kritikusság számítása:



9. ábra

A kapcsolás három fajta meghibásodási módja, illetve azok fellépési gyakorisága (alkatrész gyártóművi adat) alapján megállapított sorrend:

- 1: R ellenállás értéke megnő (0.07/év)
- 2: C kondenzátor zárlatossá válik (0.3/év)
- 3: C kondenzátor veszít a kapacitásából (0.4/év)

A következmény súlyossága:

- 1: C kondenzátor veszít a kapacitásából (hibás frekvenciamenet, működési zavarok)
- 2: R ellenállás értéke megnő (hibás frekvenciamenet, működési zavarok, szakadás esetén a szűrő működésképtelensége)
- 3: C kondenzátor zárlatossá válik (a szűrő működésképtelensége, további áramkörök esetleges üzemképtelensége)

A meghibásodás detektálhatósága:

- 1: C kondenzátor zárlatossá válik (könnyen detektálható)
- 2: R ellenállás értéke megnő (nehezebben detektálható)
- 3: C kondenzátor veszít a kapacitásából (nehezen detektálható)

A végeredmény RPN számok:

- R ellenállás értéke megnő (1x2x2=4)
- C kondenzátor zárlatossá válik (2x3x1=6)
- C kondenzátor veszít a kapacitásából (3x1x3=9)

Látható, hogy az RPN számok alapján legkritikusabb meghibásodási mód a kondenzátor kapacitás vesztése, ezt követi a kondenzátor zárlata, végül az ellenállás érték növekedése.

Másik kritikusság vizsgálati mérőszám, amikor minden komponensre definiáljuk a

$$C = \sum_{n=1}^{j} (\alpha \times \beta \times \lambda \times t)$$

számot, ahol:

α: a komponens konkrét meghibásodásának arányszáma az összes lehetséges meghibásodási módjához képest

β: az adott meghibásodási mód hatásának bekövetkezési valószínűsége

λ: az alkatrész meghibásodási rátája

t: az alkatrész működési ideje

j: az alkatrész meghibásodási módjainak a száma

A fenti aluláteresztő szűrő példája alapján a kondenzátor C értéke, amennyiben 3 év üzemidőre végezzük a vizsgálatot, valamint azt feltételezzük, hogy a zárlat 1, az értékváltozások 0.25 valószínűséggel okoznak problémát:

(0.3/(0.3+0.4)) x 1 x 0.7 x 3 + (0.4/(0.3+0.4)) x 0.25 x 0.7 x 3 = 1.20

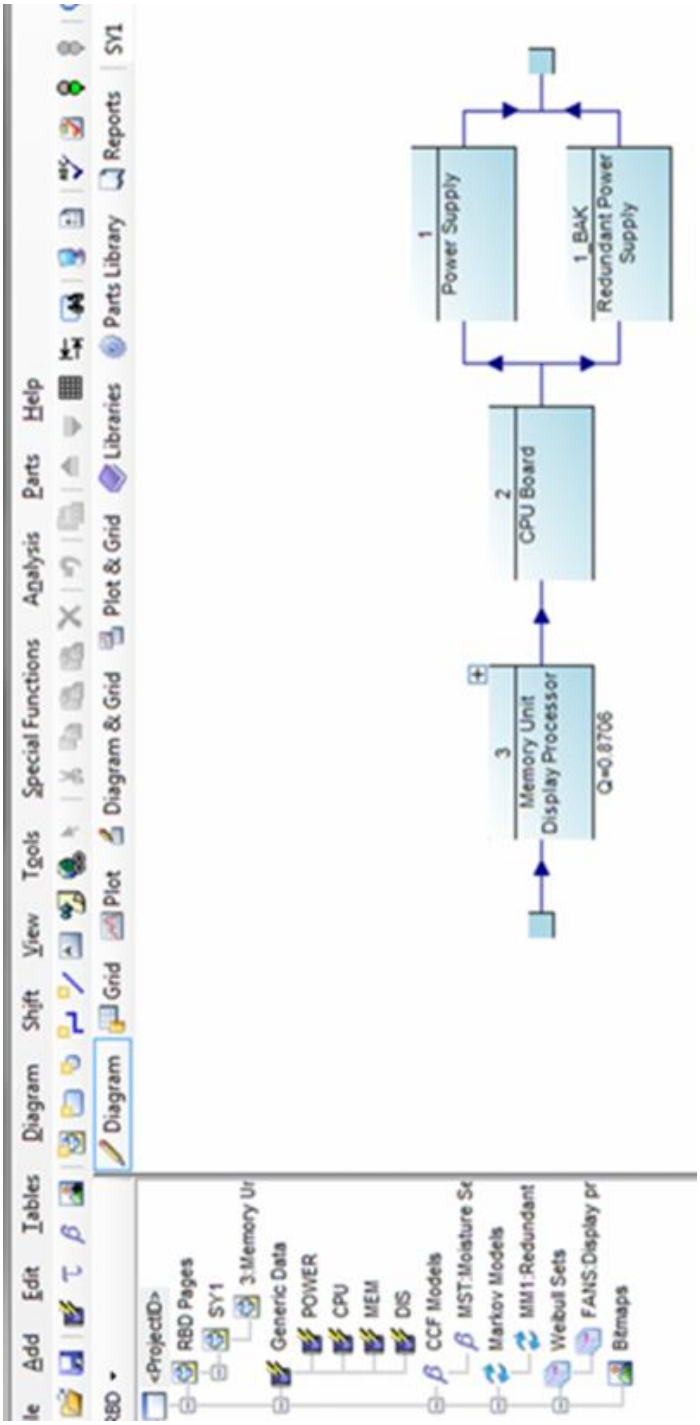
Az ellenállás C értéke:
(0.07/0.07) x 0.25 x 0.07 x 3 = 0.052, vagyis a C kritikussági szám alapján a kondenzátor meghibásodásai kritikusabbak.
A FMEA és FMECA módszerek szoftveres támogatottsága kiemelkedő a többi módszerhez viszonyítva (ReliaSoft: XFMEA, Isograph: Reliability Workbench, itemsoft: FMECA, ALD: FMECA).

Megbízhatósági tömb diagram (Reliability Block Diagram, RBD)

A megbízhatóság elemzés deduktív módszere, az **IEC (MSZ) 61078**:2006 szabvány mutatja be. Működése a hibafa módszerhez hasonlítható, annak inverze. Itt a rendszer sikeres működése a kimeneti kritérium, az ahhoz vezető logikai útvonalat ábrázolja soros-párhuzamos struktúrában. Szerkesztéséhez különféle kvalitatív módszerek használhatók.
Lépései:

- a sikeres rendszerműködés meghatározása
- a rendszer funkcionális tömbökre bontása
- további alrendszerekre való bontás (redukció)
- számszerű értékelés

Egyszerű esetben a rendszer funkcionális diagramjából megszerkeszthető, alkalmas a rendszer eredő megbízhatóságának modellezésére. Kétállapotú rendszerek esetén Boole-algebrával realizálható. A keresztirányú kapcsolatok, függőségek implementálása nehézkes, a nem definiált kimeneti állapotot nem mutatja. Nem tár fel ok-okozati utakat, az elemek időbeli működési valószínűségének ismerete szükséges.
A 8. ábrán a Reliability Workbench V11.1.1. RBD szimulációja látható, egy processzoros rendszer esetét bemutatva.
A hibátlan működéshez szükséges a memória és display modul, az alaplap, valamint valamelyik redundáns tápegység működőképessége.


File Add Edit Tables Diagram Shift View Tools Special Functions Analysis Parts Help
RBD
Diagram
Grid
Plot
Diagram & Grid
Plot & Grid
Libraries
Parts Library
Reports
SY1
<ProjectID>
RBD Pages
SY1
3:Memory Ur
Generic Data
POWER
CPU
MEM
DIS
CCF Models
MST:Moisture Se
Markov Models
MM1:Redundant
Weibull Sets
FANS:Display pr
Bitmaps
1
Power Supply
1_BAK
Redundant Power
Supply
2
CPU Board
3
Memory Unit
Display Processor
Q=0.8706

10. ábra

Megbízhatósági előrejelzés (Reliability Prediction, RP)

Induktív, előremutató módszer, a komponens adatokból számítja ki a rendszer eredő megbízhatóságát. Angol nyelvterületen alkatrész számítási módszernek is nevezik (Parts Count, PC). Az alkatrész lista összeállítása után meghatározásra kerülnek az egyes komponensek megbízhatósági rátái, igénybevétel függvényében, a tervezés korai fázisában. Majd soros rendszert feltételezve, a rendszer eredő meghibásodási rátája a komponensek meghibásodási rátáinak összege lesz. Ez a legkedvezőtlenebb eset becslését jelenti. Egyszerű, gyors megoldás, az input adatok szórása miatt kevésbé pontos. Szoftveres támogatása megfelelő, a hibák hatásmechanizmusainak kimutatására így sem alkalmas. Kritikus pontja az alkatrész meghibásodási ráta meghatározása komplex igénybevételek esetén.

Összegzés

A röviden bemutatott hat módszerrel a felsorolás közel sem teljes, a műszaki gyakorlatban még számos jól használható elemzési módszer létezik. Fenti módszerek a leggyakrabban használt, jobban ismert, szabvány által alátámasztottak. Fontos, hogy egy módszer kiválasztásakor a rendszer bonyolultságához, struktúrájához, környezeti körülményekhez, elemzési célhoz leginkább illeszkedő módszert válasszuk. Az 1. táblázat a bemutatott módszereket foglalja össze néhány praktikus szempont szerint, segítve ezzel a legalkalmasabb elemzési mód megválasztását.

Elemzési módszer	Matematikai igény	Szoftveres támogatás	Vizualitás	Előny	Hátrány	Jellemző szakterület	Információ-tartalom
FTA	közepes	közepes	jó	Struk-turált	szekvenciák, keresztkapcsolatok	űrkutatás, hadiipar, atomenergetika	jó
ETA	közepes	közepes	közepes	Struk-turált	egyenrangú események	energiaipar	közepes
Markov	közepes	közepes	közepes	Álla-pot-orien-tált	állapotszám	biztonsági rendszerek	közepes
FMEA/ FMECA	magas	magas	gyenge	Szám-szerű-ség	Idősoroza-tok	autóipar, elektronika	magas
RBD	közepes	közepes	jó	Rend-szer ana-lógia	ok-okozati utak	számítás-technika	jó
RP	alacsony	alacsony	gyenge	Egy-szerű, gyors	pontatlan	korai tervezés	közepes

6. táblázat

Felhasznált irodalom

[1] 2/2001. (I. 17.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

[2] IEC (1990), Standard IEC 1025 Fault tree analysis (FTA), International Electrotechnical Commission, 39.

[3] MMBH/MBF: Seveso füzetek 1-5

[4] Johanyák Zsolt Csaba: Hibafa elemzés a hibátlan tervezés érdekében

[5] Prímagáz Hungária Rt: Nyilvános biztonsági jelentés

[6] dr. Majzik István: Veszély- és kockázati analízis

[7] Szabó Géza: Bevezetés a hibafa analízisbe

[8] www.isograph-software.com

[9] Ajtonyi István- Gyuricza István: Programozható irányítóberendezések, hálózatok és rendszerek

[10] Szabó Géza: Műszaki okú kockázatok kezelése a közlekedésben

[11] http://www.2ge.hu/doc/

[12] Szabó Géza: Nagy megbízhatóságú elektronikus közlekedési alrendszerek RAMS paramétereinek kezelése Ph.D értekezés

[13] Lendvay Marianna–Zsigmond Gyula : Komplex villamos rendszerek megbízhatóság-elemzési módszerei

[14] Schutzbach Mártonné: Az informatikai rendszerek biztonságának kockázatelemzése a védelmi szférában

[15] Pokorádi László: Mátrixalgebrai hibafa-érzékenység elemzés

[16] Dr Rajnai zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23.

Solymosi János[32]: Kockázatértékelés a munkavédelemben risk assesment in Occupational health and safety (OHS)

Absztrakt
*A **kockázatelemzés** a lehetséges kockázatok azonosítása, csoportosítása és értékelése egy jelenségnél vagy folyamatnál. Ennek során vizsgálják a kockázatok bekövetkezési valószínűségét, okozott hatását, illetve a kockázat bekövetkeztének elkerülésére, illetve hatásának csökkentésére teendő intézkedéseket.*
Az elemzés végeredményeképpen kidolgozásra kerülnek a lehetséges kockázatcsökkentő intézkedések. Így történik ez a munkavédelemben is. Jelen publikáció a munkavédelmi kockázatértékelés szükségességét, módszertanát, folyamatát kívánja megvilágítani.

Abstract
The risk analysis is the identification, classification and assessment of potential risks at phenomena or processes. Examine the probability of occurrence of risks in doing so, caused the effect, or to prevent the risk from occurring, or to reduce the impact of measures to be taken.
The end result of this analysis will be developed in the possible risk reduction measures. Thus, this work is done well protected. This publication intends to highlight the need for health and safety risk assessment methodology and process.

1. Bevezetés

A Wikipédia szabad enciklopédia szerint a kockázat valamely cselekvéssel járó veszély, veszteség lehetősége.[1] Ha belegondolunk életünknek nincs olyan területe, ahol valamilyen kockázattal ne kellene számolnunk. A magánélettől kezdve a gazdasági-társadalmi folyamatokig bizonyos kockázattal mindenütt találkozunk. Az ember (és az állat is) születésétől kezdve végez előbb ösztönös, majd tudatos kockázatelemzést és kockázatértékelést. Minél több ismerettel rendelkezünk a várható kockázatokra vonatkozóan, annál jobban felkészülhetünk azok veszélyeinek kezelésére vagy elhárítására.

Kockázat mindig van, csak azt kell megállapítani, hogy annak mértéke elfogadható, tűrhető, vagy elfogadhatatlan-e. A kockázatelemzés a lehetséges kockázatok számbavétele, csoportosítása és értékelése a figyelemmel kísért jelenséggel, vagy folyamattal kapcsolatban. Az elemzés a lehetséges kockázatcsökkentő intézkedések

[32] Az Óbudai Egyetem Biztonságtudományi Doktori Iskola Ph.D hallgatója sojanos1@t-online.hu

kidolgozásával zárul, az elérni kívánt cél a minimális kockázat. A kockázatkezelés a kockázatpotenciál csökkentését jelenti kármegelőzéssel, vagyis a várható negatív esemény bekövetkezési valószínűségének csökkentésével (ez a prevenció), ill. kárcsökkentéssel, a kárhatás horderejének ellensúlyozásával (ez a korrekció).

2. Néhány szó a munkavédelemről

Először is tisztázandó: mit is kell védeni? Pusztán nyelvtanilag elemezve a „munkavédelem" szót, arra a következtetésre jutnánk, hogy a munkát (?). Pedig erről szó sincs, hiszen a munkavédelem: a szervezett munkavégzésre vonatkozó munkabiztonsági és munkaegészségügyi követelmények, továbbá törvénykezési, szervezési, intézményi előírások rendszere, valamint mindezek végrehajtása. [1] Úgy is lehet fogalmazni, hogy a munkát végző személyt kell védeni a testi épségét és egészségét veszélyeztető környezeti káros hatásoktól a munkahelyeken. Megjegyzem, ha elvonatkoztatunk a munkavédelemre vonatkozó jogszabályi előírásoktól ez a környezeti károsító hatásoktól történő védelem biztosítása elemi érdeke minden munkát végző személynek, függetlenül attól, hogy szervezett vagy nem szervezett munkavégzésről van-e szó. Jogi értelmezés szerint akkor beszélünk szervezett munkavégzésről, ha annak ismérvei a munkavégzés során fellelhetők. Ezek (a teljesség igénye nélkül) a következők:

- szerződéses jogviszony a munkáltató és a munkavállaló között
- a munkavégzés ellentételezés fejében történik
- fennáll az alá-fölérendeltség a munkavállaló és a munkáltató között
- a munkaeszközöket a munkáltató biztosítja a munkavállaló számára, stb.

Ezek az ismérvek nincsenek meg például az otthon, saját érdekben végzett, vagy a szomszédi illetve baráti segítségként végzett munka esetén, azonban a munkát végző testi épségét és egészségét ilyen esetekben is óvni kell a károsodásoktól. A munkahelyeken a munkavállaló testi épségének károsodása másnéven a munkabaleset, egészségének a károsodása a foglalkozási megbetegedés. Alapvető különbség a kettő között a bekövetkezés időtartama. Míg a munkabaleset hirtelen vagy viszonylag rövid idő alatt következik be, addig a foglalkozási megbetegedés kialakulása hosszú idő – *akár több év* – alatt alakul ki.

A munkabalesetnél a hirtelen vagy viszonylag rövid idő alatti bekövetkezés magyarázatára lássunk két példát:

- Az ács egy épülő ház tetőjéről, 6 m magasból lezuhant, többszörös csonttöréses balesetet szenvedett el. Az esemény hirtelen és váratlanul következett be, a zuhanás ideje „mindössze" 0,7 másodperc.
- A takarítónő mosdó tisztítása során összekeverte a sósavat a hypoval, az anyagok reakciója során keletkezett gázt belélegezte. Először csak köhögött, kaparást érzett a torkában, majd egyre nehezebben tudott lélegezni. Öt perc elteltével mentővel kórházba kellett szállítani.

A második eset is balesetnek minősül, mert a heveny egészségkárosodás pár perc alatt bekövetkezett. Ha netalán ugyanez a dolgozó egy vegyianyag raktárban több éven keresztül lélegezett volna be egyszerre viszonylag kisebb mennyiségű, légzést károsító gázt, akkor már foglalkozási megbetegedés kialakulásáról beszélhetnék. A munkavédelem két nagy alkotó részterülete a munkabiztonság és a munkaegészségügy. mindkét részterület külön szakmát képvisel, nem véletlen, hogy a jogszabály egyes munkavédelemmel kapcsolatos tevékenységet munkabiztonsági és/vagy munkaegészségügyi szaktevékenységként emleget. Ez azt jelenti, hogy ezek a szaktevékenységek csak megfelelő szakképesítés birtokában végezhetők. Ilyen tevékenységnek minősül többek között a munkahelyi kockázatértékelés is.

3. A munkahelyi kockázatértékelés specifikuma

A kockázatértékelést széles körben alkalmazzák az állami- és magánágazatokban (állami intézmények, bankok, biztosítótársaságok, szoftveripar, piackutató cégek, gyártó cégek, stb.) különböző tevékenységekre. A kockázatértékelés célja valamilyen érdek maximális módon történő érvényesítésére törekvés, ezen belül a kockázatok elhárítása, illetve elfogadható mértékűre csökkentése. Általában minden fentebb említett ágazatban a cég érdek (gazdasági érdek) érvényesítése áll a középpontban.
A kockázatok formái lehetnek:

- Stratégiai kockázatok (pl. stratégia hiánya, vagy nem megfelelő volta, vagy nem megfelelő végrehajtása, alkalmazása következményei, …)
- Pénzügyi kockázatok (pl. pénzáramlás nem megfelelő tervezése, akadályoztatása, kinnlévőségek kezelése, likviditási problémák)
- Piaccal és vevővel kapcsolatos kockázatok (pl. termék értékesítési gondok, piaci igények ill. piaci szegmens változása, stb.)
- Jogi kockázatok (pl. törvényi nem-megfelelés, hatósági engedélyeztetési kockázatok, szerződéses kötelezettségek teljesíthetősége, stb.)

  - Működési kockázatok (folyamatok működésével, termelési minőséggel, üzemeltetéssel, munka- és tűzvédelemmel, környezetvédelemmel, stb. összefüggő kockázatok)
  - Személyi kockázatok (pl. személyi állománnyal, kulcsemberek kiválasztásával ill. teljesítményével összefüggő problémák)

Jellemző kockázati területek:

- Piaci kockázatok
- Nem megfelelő marketing módszerek kockázatai
- Ajánlatadási kockázatok
- Projektkockázatok
- Beruházások kockázatai
- Fejlesztések kockázatai
- Folyamatszervezés kockázatai
- Termelés – hibakockázatok
- Karbantartási kockázatok
- Cash-flow kockázatok
- Befektetési kockázatok
- Likviditásai kockázatok
- BCP – DRP
- Környezetvédelmi kockázatok
- Munka- tűzvédelmi kockázatok
- Információbiztonsági – IT működési kockázatok
- Egyéb biztonsági kockázatok
- Környezeti kockázatok
- Személyek képzettségével (vagy érdekeltségével – ellenérdekeltségével) összefüggő kockázatok
- Beszállítói minőség kockázata, stb.

Mindegyik terület kockázatainak megvan a saját jellemző, szakmai értékelési és kezelési eljárása.[2] A munkavédelem is az egyik jellemző kockázati terület a cégek életében, azonban ki kell emelnünk, hogy a munkavédelmi kockázatértékelés, mindamellett hogy van ilyen vonzata is, *nem* elsősorban gazdasági érdekérvényesítés, hanem az *emberi élet és egészség védelme* érdekében tett intézkedés, érdekérvényesítés.

4. Munkavédelmi szempontú kockázatértékelés a munkahelyeken

A munkavédelemről szóló 1993. évi XCIII. törvény (továbbiakban törvény) alapján az egészséget nem veszélyeztető és biztonságos munkavégzés érdekében a munkáltató köteles figyelembe venni a következő általános követelményeket:

- a veszélyek elkerülése;
- a nem elkerülhető veszélyek értékelése;
- a veszélyek keletkezési helyükön történő leküzdése;
- az emberi tényező figyelembevétele a munkahely kialakításánál, a munkaeszközök és munkafolyamat megválasztásánál, különös tekintettel az egyhangú, kötött ütemű munkavégzés időtartamának mérséklésére, illetve káros hatásának csökkentésére, a munkaidő beosztására, a munkavégzéssel járó pszichoszociális kockázatok okozta igénybevétel elkerülésére;
- a műszaki fejlődés eredményeinek alkalmazása;
- a veszélyes helyettesítése veszélytelennel vagy kevésbé veszélyessel;
- egységes és átfogó megelőzési stratégia kialakítása, amely kiterjed a munkafolyamatra, a technológiára, a munkaszervezésre, a munkafeltételekre, a szociális kapcsolatokra és a munkakörnyezeti tényezők hatására;
- a kollektív műszaki védelem elsőbbsége az egyéni védelemhez képest;
- a munkavállalók megfelelő utasításokkal történő ellátása.[3]

Kockázatértékelési kötelezettség

A munkáltatók kockázatértékelési kötelezettségét írja elő. A törvény úgy rendelkezik, hogy a munkáltatónak rendelkeznie kell kockázatértékeléssel, amelyben köteles minőségileg, illetve szükség esetén mennyiségileg értékelni a munkavállalók egészségét és biztonságát veszélyeztető kockázatokat, különös tekintettel az alkalmazott munkaeszközökre, veszélyes anyagokra és keverékekre, a munkavállalókat érő terhelésekre, valamint a munkahelyek kialakítására. A kockázatértékelés során a munkáltató azonosítja a várható veszélyeket (veszélyforrásokat, veszélyhelyzeteket), valamint a veszélyeztetettek körét, felbecsüli a veszély jellege (baleset, egészségkárosodás) szerint a veszélyeztetettség mértékét. A kockázatértékelés során az egészségvédelmi határértékkel szabályozott kóroki tényező előfordulása esetén munkahigiénés vizsgálatokkal kell gondoskodni az expozíció mértékének meghatározásáról. A munkáltató a kockázatértékelést, a kockázatkezelést és a megelőző intézkedések meghatározását

a tevékenység megkezdése előtt köteles elvégezni. Az első kockázatértékelést követően kockázatértékelést kell végezni:

- legalább 3 évente,
- ha az alkalmazott tevékenység, technológia, munkaeszköz, munkavégzés módja megváltozik, illetve minden olyan, az eredeti tevékenységgel összefüggő változtatás esetén, amelynek eredményeképpen a munkavállalók egészségét, biztonságát meghatározó munkakörülményi tényezők megváltozhattak – ideértve a munkaklíma-, zaj-, rezgésterhelést, légállapotokat (gázállapotú, por, rost légszennyezők minőségi, illetve mennyiségi változását).

Soron kívül kell kockázatértékelést végezni, ha az alkalmazott tevékenység, technológia, munkaeszköz, munkavégzés módjának hiányosságával összefüggésben munkabaleset, fokozott expozíció következett be, illetve foglalkozási megbetegedés fordult elő, vagy a kockázatértékelés valamilyen munkahelyi kockázatra nem terjedt ki. Megjegyzem, azoknál a cégeknél ahol MEBIR-t (Munkahelyi Egészségvédelem és Biztonság Irányítási Rendszere) működtetnek az MSZ 28001:2008 szabvány előírja a munkahelyekre vonatkozó veszélyazonosítást, kockázatértékelést és a kockázatok kézbentartását.

Fogalmak (a törvény szerint)

- Munkahely: minden olyan szabad vagy zárt tér (ideértve a föld alatti létesítményt, a járművet is), ahol munkavégzés céljából vagy azzal összefüggésben munkavállalók tartózkodnak.
- Munkaeszköz: minden gép, készülék, szerszám vagy berendezés, amelyet a munkavégzés során alkalmaznak vagy azzal összefüggésben használnak
- Veszélyes: az a létesítmény, munkaeszköz, anyag/készítmény, munkafolyamat, technológia (beleértve a fizikai, biológiai, kémiai kóroki tényezők expozíciójával járó tevékenységeket is), amelynél a munkavállalók egészsége, testi épsége, biztonsága megfelelő védelem hiányában károsító hatásnak lehet kitéve.
- Veszélyforrás: a munkavégzés során vagy azzal összefüggésben jelentkező minden olyan tényező, amely a munkát végző vagy a munkavégzés hatókörében tartózkodó személyre veszélyt vagy ártalmat jelenthet.
- Kockázat: a veszélyhelyzetben a sérülés vagy az egészségkárosodás valószínűségének és súlyosságának együttes hatása.
- Megelőzés (prevenció): a munkáltató által megtett vagy tervezett intézkedések a munkáltatói tevékenység bármely fázisában, amelyeknek célja a munkával összefüggő kockázatok megelőzése vagy csökkentése.

- Munkahigiénés vizsgálatok: a munkakörnyezetben lévő kóroki (fizikai, kémiai, biológiai, ergonómiai, pszichoszociális) tényezők feltárására, szintjének, továbbá a végzett munkából és a munkakörnyezet hatásaiból adódó megterhelés mennyiségi meghatározására alkalmas eljárások, valamint olyan vizsgálatok, amelyek eredményeként javaslat tehető a munkából és a munkakörnyezetből származó egészségkárosító kockázatok kezelésére (csökkentésére).

A kockázatértékelés menete

A kockázatértékelést egyéni védőeszköz nélküli, szabályos munkavégzésre, munkahelyekre technológiákra szükséges és indokolt elkészíteni. A kockázatértékelés első lépéseként el kell végezni a veszélyek azonosítását a munkahelyeken. A következő feladat a veszélyeztetettek azonosítása, az érintettek számának meghatározása. Fel kell mérni a kockázatot súlyosbító tényezőket is. Ezután következik a kockázatok minőségi, illetőleg mennyiségi értékelése, a fennálló helyzettel való összevetés alapján annak megállapítása, hogy a körülmények megfelelnek-e a munkavédelemre vonatkozó szabályoknak, illetve biztosított-e a kockázatok megfelelően alacsony szinten tartása. A mennyiségi értékelés azt jelenti, hogy amennyiben szükséges különböző méréseket is el kell végezni ahhoz, hogy a tényleges kockázatok hatásmechanizmusát követni tudjuk. A tények és az előírások összevetését követően a szükséges megelőző intézkedéseket meg kell határozni a végrehajtási határidő (ütemterv) és a felelősök megjelölése mellett. A munkahelyi kockázatértékelést dokumnetáltan kell elvégezni. Az írásos dokumentumnak – *a fentiek mellett* – tartalmaznia kell a kockázatértékelés időpontját, helyét és tárgyát, az értékelést végző azonosító adatait, a kockázatértékelés elkészítésének tervezett következő időpontját és az előző kockázatértékelés időpontját. A dokumentumot legalább öt évig meg kell őrizni. A kockázatértékelés eredményéről tájékoztatni kell a munkahelyi vezetést, az érintett munkavállalókat, a munkahelyi érdekképviseletet. A kockázatértékelésre formai és módszertani követelmények nincsenek.

Veszélyforrások csoportosítása

Fizikai veszélyforrások:

- munkaeszközök, járművek, szállító-, anyagmozgató eszközök, ezek részei, illetve mozgásuk, termékek és anyagok mozgása,
- szerkezetek egyensúlyának megbomlása,
- csúszós felületek,
- éles, sorjás, egyenetlen felületek, szélek és sarkok,
- tárgyak hőmérséklete,

- a munkahelynek a föld (padló) szintjéhez viszonyított elhelyezése,
- szintkülönbség,
- súlytalanság,
- a levegő nyomása, hőmérséklete, nedvességtartalma, ionizációja és áramlása,
- zaj, rezgés, infra- és ultrahang,
- világítás,
- elektromágneses sugárzás vagy tér,
- részecskesugárzás,
- elektromos áramköri vagy sztatikus feszültség,
- aeroszolok és porok a levegőben

Nézzünk a fentebb felsoroltakra példákat a jobb érthetőség érdekében. Munkaeszközök, járművek, szállító-, anyagmozgató eszközök és részei mozgásából adódó veszélyek: elütés, fellökés, összenyomás, elsodrás, elgázolás, átszúrás. Egy mozgó jármű – ugyanúgy mint a közlekedés bármely területén – az előzőleg említett veszélyeket mind magában rejti. Szállító-, anyagmozgató eszköznél megemlíthetjük a híddarut, amely megemelt teherrel haladva az ellökés, ráejtés, összenyomás, elvágás veszélyét hordozhatja magában. Szabálytalan anyagtárolás esetén az egymásra rakott darabáru, a szabálytalanul felhalmozott ömlesztett anyag egyensúlyának megbomlásakor az anyag eldőlése, rakat összeborulása, ömlesztett anyag váratlan omlása az elütés, ráborulás, betemetés veszélyét jelentheti a helyszínen tartózkodó személyek számára. A csúszós felületekre jó példa az olajjal szennyezett vagy jéggel borított járófelület, amely az azon közlekedő járművek számára a megcsúszás, ütközés, a személyek esetében az elesésből származó baleset lehetőségét foglalja magába. A megmunkált munkadarabok éles, sorjás felületei (pl. sajtológépen sajtolt lemez munkadarab) a kéz és más testrész vágásos, karcolásos, horzsolásos sérülését okozhatják. Egyenetlen felületre jó példa lehet az egyenetlen járófelület, amely a botlás, esés veszélyével jár. ki ne ütötte volna már be a combját az asztal sarkába? Az asztal sarka figyelmetlen közlekedés során a beütés, zúzódás veszélyét hordozza. A tárgyak szélsőséges (túl hideg vagy túl meleg) hőmérséklete jelent elsősorban veszélyforrást. A túl hideg felület fagyásveszélyt, a túl meleg (60 C^{o} feletti) pedig égési veszélyt jelent. A hideg felületre példa lehet a hűtőházi munkák során a fagyasztott termékek kezelése, a meleg felületre pedig az úgynevezett „fekete meleg” alkatrészek felületi hőmérséklete kovácsolási művelet után. A munkahelynek a föld (padló) szintjéhez viszonyított elhelyezésére jó példa a csővezetékek fektetéséhez alkalmatott különböző mélységű (0,8-6 m) föld munkaárok, amelyeknél a beesés veszélye áll fenn. A szintkülönbség, mint

veszélyforrás jelentkezik például a tetőépítésnél az ácsoknál, akik a talajhoz viszonyított 5-10 m magasságban végzik munkájukat és megfelelő védelem hiányában leesés veszélye áll fenn. A súlytalansággal mint veszélyforrással Magyarországon a polgári életben nem kell számolnunk. A levegő nyomása, nedvességtartalma, ionizációja a magyarországi klímaviszonyokat alapul véve nem jelentkezik számbaveendő veszélyforrásként, a hőmérséklete és áramlása viszont annál inkább. A levegő magas hőmérséklete az emberi szervezet folyadékveszteségét okozza, a folyadékpótlás hiánya esetén a szervezet sokkos állapotba kerülhet, amit a koncentrációképesség romlása, fejfájás előz meg. Hidegben, szélsőséges esetben a szervezet működése lelassulhat, a kihűlés veszélye is jelentkezhet. A fokozott levegőáramlásra (huzatra) az emberi szervezet egyéni érzékenységtől függően reagál, megbetegedést okozhat. A zajos környezetben végzett huzamos idejű munka halláskárodsodást okozhat, a károsító hatást befolyásolja a hang frekvenciája (magassága) valamint intenzitása is. A halláskárosító hatása mellett károsan befolyásolhatja a zajos helyen dolgozó munkavállaló pszihéjét is (egy idő elteltelte után ingerültté válik, feje fáj, stb.). Ugyanakkor ha egy hang nem elég intenzív, szintén veszélyforrásként jelentkezhet. (például ha a vészhangjelzést elnyomja környezeti zaj) A rezgés a munkavállalók izületeit veszi igénybe intenzíven. A világításnál szintén veszélyforrásként értékelendő mind a túlzott, mind az elégtelen megvilágítás. A túlzott megvilágítás káprázást okoz, vakít, ehhez párosulhat még a nem megfelelő árnyékhatás. A nem elegendő megvilágítottság miatt egyéb veszélyforrások észlelése maradhat el. Az elektromágneses terek sugárzások egészségkárosító hatása még orvosi körökben sem tisztázott kellően, azonban feltételezik, hogy huzamos időn keresztül mágneses térben tartózkodva a nemzőképesség károsdhat. A részecskesugárzások egészségkárosító hatását nem kell különösebben részletezni, ha Hirosmára vagy Csernobilre gondolunk. Az elektromos áramköri vagy sztatikus feszültség veszélye közül az áramütés veszélyét kiemelve közismert tény, hogy az akár halálos kimenetelű is lehet, azonban a sztatikus feszültség veszélyét kevesen ismerik. A sztatikus feszültség olyan áramütést nem okoz, melynek súlyos élettani következményei lennének, azonban csípő érzést okoz, ezért úgynevezett másodlagos baleset okozója lehet. Ezt egy példán keresztül illusztrálom. Tételezzük fel, hogy a dolgozó 4 méter magasban létráról végez valamilyen műveletet, úgy hogy a teste, ruházata sztatikusan fel van töltődve és a tevékenysége során hozzáér egy földelt acélszerkezethez. A kezén úgy érzi, mintha áramütés érte volna, azonban ténylegesen csak a testén felhalmozódott villamos töltések távoztak a földelt acélszerkezeten keresztül. A csípő érzés hatására a létrával eldől, és az esés következményeként alkarja eltörik. Azaz a baleset nem a sztatikus kisülésnek,

hanem az esésnek a közvetlen következménye. Aeroszolok és porok a levegőben légzőszervi megbetegedéseket, rákot (keményfa por), ha pedig mérgező anyagok aeroszoláról vagy poráról van szó még mérgezést is okozhatnak.

Veszélyes anyagok

Minden anyag vagy készítmény, amely fizikai, kémiai vagy biológiai hatása révén veszélyforrást képviselhet, így különösen a

- robbanó,
- oxidáló,
- gyúlékony,
- sugárzó,
- mérgező,
- maró,
- ingerlő,
- szenzibilizáló,
- fertőző,
- rákkeltő,
- mutagén,
- teratogén,
- utódkárosító (beleértve a spontán vetélést, koraszülést és a magzat retardált fejlődését is),
- egyéb egészségkárosító
- anyag.

A munkahelyeken használt veszélyes anyagokra vonatkozó információkat a biztonsági adatlapok tartalmazzák.

Biológiai veszélyforrások:

- mikroorganizmus (vírus, baktérium) és anyagcsereterméke
- makroorganizmus (növény, állat)

Fiziológiai, idegrendszeri és pszichés igénybevétel: Ezek körébe sorolható az ergonómiailag nem tervezett munkahely, természetellenes testtartás, monoton munkavégzés, teljesítmény kényszer alatt végzett munka, munkavállalók egymás közötti konfliktusai, vezetők és beosztottak közötti konfliktusok, stb.

A veszélyek azonosítása

A munkahelyeken részletesen számba kell venni a munkakörnyezetben lévő valamennyi munkafolyamatot, technológiát, munkaeszközt, felhasznált anyagokat

(különös tekintettel a veszélyes anyagokra és készítményekre) és munkamódszert. Rendkívül fontos, hogy ez kiterjedjen a nem mindennapos tevékenységekre is, mint például a karbantartás. Emellett figyelemmel kell lenni egyes munkafeladatok évszakhoz kötött jellegére is, valamint gondot kell fordítani a kisegítő jellegű tevékenységekre, mint például a takarítás, anyagtárolás vagy szemétszállítás.
Ezután kell meghatározni minden jelenlevő veszélyt, amely a munkavállalókat és más személyeket fenyegethet. Ezeket lehet a tevékenységek, a technológiák, a hely, vagy más alkalmas szempont szerint osztályozni, azonban mindig úgy, hogy minden lényeges veszély számba legyen véve. A veszélyek sokféle módon előfordulhatnak, ezért előfordulási tényezőt figyelembe kell venni.

A veszélyek azonosításához információt lehet gyűjteni:

- A munkatevékenység, munkafolyamatok, technológiák, munkaeszközök, munkamódszerek közvetlen megfigyelése
- A munkavállalók és képviselőik tapasztalatainak összegyűjtése
- Munkavédelmi jogszabályok tanulmányozása
- Szabványok tanulmányozása
- Gyártók és szállítók használati utasításai, adatlapjai, gépkönyvei, kezelési utasításai tanulmányozása
- Munkahelyi belső szabályzatok, üzemeltetési dokumentáció átvizsgálása
- Munkabalesetek, foglalkozási megbetegedések és rendkívüli események elemzése
- Más, hasonló munkahelyek közzétett adatai, tapasztalatai, bevezetett szakmai szokásai
- Tudományos és műszaki irodalom tanulmányozása
- Munkavédelmi adatbázisok elemzése
- Helyszíni vizsgálatok, mérések
- Szaktanácsadók, munkavédelmi szolgáltatók veszélyazonosítási tapasztalatai alapján.

A veszélyeztetettek azonosítása, az érintettek száma

A lehető legteljesebb körben figyelembe kell venni azokat a személyeket, akiket az azonosított veszélyek fenyegetnek, így a munkahelyen foglalkoztatott azon munkavállalókat, akik folyamatosan ott végzik a munkájukat, illetve azokat is, akik az adott munkahelyen rendszeresen megfordulnak (például anyagfeltöltők). A veszélyeztetettek azonosításánál figyelembe kell venni azokat a személyeket is, akik alkalomszerűen lehetnek jelen az adott munkahelyen (látogatók, auditorok, üzletfelek, stb.) Figyelembe kell venni azt is, hogy az adott munkahelyen dolgoznak/dolgozhatnak-e nők, fiatalkorúak, megváltozott munkaképességűek. Az

érintettek számának meghatározása azért fontos, mert a kockázat mértéke a veszélyeztetettek számával arányban áll.

A kockázatok minőségi és mennyiségi értékelése

Az értékelés során figyelembe kell venni egyrészt a veszély súlyosságát, vagyis a kockázatok manifesztálódása esetén bekövetkezhető kár mértékét és kiterjedését, ideértve a veszélyeztetettek számát is, másrészt a veszély okozta károsodás bekövetkezésének valószínűségét. A besorolás alapja lehet például a lehetséges károsodás jellege, súlyossága (anyagi kár, kisebb személyi károsodás, súlyos személyi károsodás, halálos baleset) és az érintettek száma. Belátható, hogy nem egyenrangú egy vagy több ember egy időben bekövetkezett sérülése, mint ahogy az sem, hogy csupán horzsolásos bőrsérülést szenvednek el, vagy elveszítik érzékszervüket, testrészüket egy munkahelyi baleset esetén. Egy károsodás bekövetkezésének valószínűsége azonos veszélyek mellett más lehet egy olyan munkahelyen, ahol betartják a munkavédelemre vonatkozó biztonsági előírásokat, megfelelő szakképzettséggel, jártassággal bíró, egészségileg alkalmas, fegyelmezett munkavállalók dolgoznak, mint ahol mindez nem így van.

A veszélyeztetés, a súlyosság mértékének és fokozatának neghatározását az alábbi 1. sz. táblázat szerint is végezhetjük:

Fokozat	Súlyosság mértéke	Hatás
5	katasztrofális	Halállal végződő tömeges balesetek, betegségek, berendezések, épületek nagymértékű károsodása, nagy területre kiterjedő vészhelyzeti jellegű események.
4	kritikus	Halálos baleset, betegségek súlyos sérülésekkel és tartós következményekkel, maradandó egészségkárosodással.
3	közepes	Balesetek, betegségek tartós következmények nélkül, hosszú ideig tartó betegállománnyal. Épületek, berendezések viszonylag alacsony anyagi károsodása.
2	mérsékelt	Balesetek, betegségek enyhébb sérülésekkel, rövid ideig tartó betegállomány, sérülések. Berendezések, épületek anyagi károsodása elhanyagolható.
1	kicsi	Nincs sérülés, vagy jelentéktelen apró sérülések, betegállományt nem igényelnek. Anyagi károsodás nincs.

1.sz. táblázat

A negatív hatás bekövetkezésének a valószínűsége besorolható a 2. táblázat alapján is.

Fokozat	**Valószínűség**
5	valószínűsíthető, előre látható
4	nagyon valószínű
3	közepesen valószínű
2	alig valószínű
1	valószínűtlen

2. sz. táblázat

A veszélyeztetett létszám alapján meghatározható az azzal kapcsolatos fokozat a 3. táblázat szerint:

Fokozat	Létszám
3	10 fő felett
2	3-5 fő között
1	1-2 fő

3. sz. táblázat

A kockázati szintet a kockázat mértéke alapján meghatározhatjuk. A kockázat mértéke az 1. 2. és 3. sz. táblázat alapján a súlyossági fokozat, a valószínűségi fokozat és a létszám fokozat alapján határozható meg, a három szám szorzata. Egy közepes súlyosságú (3), közepesen valószínű (3), 4 főt érintő (2) veszély esetén ez a szám 18.

A kockázati szintet határozzuk meg a 4. táblázat szerint:

Kockázati érték	Kockázati szint
1-12	nem jelentős
13-47	jelentős
48-75	elviselhetetlen

4. sz. táblázat

A táblázat értékei önkényesen lettek meghatározva, a kockázatértékelést végző más fokozati és kockázati értéket is meghatározhat, egyéb tényezőket is figyelembe vehet, ugyanis mint azt fentebb is említettem a munkahelyi kockázatértékelésnek nincsenek formai és módszertani kötelmei. A kockázatok minőségi, illetőleg mennyiségi értékelése során a munkáltatónak el kell döntenie, hogy:

- a jelenlegi helyzet kielégíti-e a munkavédelemre vonatkozó jogszabályi követelményeket,
- a kockázatok megfelelő ellenőrzés alatt állnak-e,
- a jelenlegi kockázatok megszüntethetők-e, és miként,
- milyen intézkedéseket kell tenni a kockázatok megelőzése vagy csökkentése érdekében.

A szükséges intézkedések meghatározása a kockázatok minőségi és mennyiségi értékelése után

A szükséges intézkedések meghatározásához elsődlegesen azt kell megállapítani, hogy az adott munkafolyamat, technológia, anyag, munkaeszköz hogyan tehető biztonságosabbá, valamint hogy milyen munkavédelmi intézkedések szükségesek a kockázatok alacsony szinten tartásához. Ehhez az alábbi lehetőségeket szükséges számba venni:

- a veszély keletkezési helyén történő felszámolása: zárt technológia alkalmazása, elszívás, hőszigetelés, zajcsökkentés, stb.,
- a munkafolyamat, technológia elkülönítése, elszigetelése,
- a munkavállaló eltávolítása a veszélyes munkafolyamattól,
- a munkaeszközök ellátása biztonsági berendezéssel, például védőburkolattal, biztonsági indítással, vészleállítóval,
- megfelelő mozgástér biztosítása,
- munkahelyi rend és tisztaság, szabályos anyag-, szennyvíz-, hulladékkezelés,
- a munkavállalók megfelelő tájékoztatása, képzése, oktatása, ellenőrzése,
- megfelelő jelző- és riasztóberendezések, mentési tervek, menekülési útvonalak és elsősegély,
- kellő szakképzettségű és számú munkavállaló alkalmazása,
- munkaszervezés, a munka összehangolása,
- rendszeres, tervezett karbantartás megszervezése,
- veszélyes technológiák és munkaeszközök időszakos biztonsági felülvizsgálata,
- egyéni védőeszközök biztosítása
- a foglalkoztatás egészségügyi feltételeinek biztosítása [4]

A szükséges intézkedések meghatározását követően intézkedési tervet kell készíteni végrehajtási határidő és felelős meghatározásával. A végrehajtást folyamatosan ellenőrizni kell. A törvény ugyan előírja, hogy alapesetben három évente kockázatértékelést kell végezni a munkahelyeken.

Összegzés

Belátható, hogy a kockázatértékelés egy folyamat, nincs eleje és vége, hanem folyamatosan kell végezni ahhoz, hogy a munkavállalók és a munkáltatók közös érdeke: a sérülések és megbetegedések megelőzése teljesüljön.

Felhasznált irodalom

[1] http://hu.wikipedia.org/wiki/Kock%C3%A1zat
[2] http://www.slideshare.net/HZsolt/kockzatrtkels-kerekasztal
[3] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99300093.TV (1993. évi XCIII. törvény a munkavédelemről
[4] http://munkaugyilevelek.hu/2006/11/kockazatertekeles-a-munkahelyen/

Szabó Anna[33]: Az Európai Unió és Amerikai Egyesült Államok adatvédelmi megközelítésből

Absztrakt
Az Amerikai Egyesült Államok (továbbiakban: USA) adatvédelme nem egységes, tartományonként eltérő, ezzel szemben az Európai Unió célja egységes jogrendszer megalkotása és alkalmazása mind a 28 tagországban, melyet a csatlakozási eljárás során a tagjelölt országoknak is be kell ültetniük a saját jogrendjükbe. Az USA-ban sokszor nagyobb jelentőséget tulajdonítanak a vélemény nyilvánítás és a sajtó szabadságának, mint az egyén információs önrendelkezési jogának. Ez megnehezíti azon jogi eljárásokat, melyeket egy európai állam indít egy amerikai szolgáltató által üzemeltetett weboldal tartalma ellen. Másrészről a nemzetközi kereskedelem folytatása és a személyszállítás során a terrorizmustól való félelem jegyében az USA előszeretettel végez az uniós jogrendszer szerint indokolatlan, vagy nem megfelelően végrehajtott adatgyűjtést, ami sérti az Európai Unió által elfogadott emberi jogokat. A téma aktualitása miatt a cikkben az Európai Unió és az USA adatvédelmi rendelkezéseit fogom összehasonlítani.

Abctract
This article shows some quetions about EU, and US Privacy.

1. Történelmi áttekintés

A két hatalmi tényező közötti ellentét már magában a jogrendszereik alakulásában, fejlődésében fellelhető. Ugyanis Európában jellemzően a kontinentális jogrendszer érvényesül, mely jellegzetessége a kodifikáció, az írott jog túlsúlya a bírói joggyakorlattal szemben, ez alól kivétel Nagy-Britannia jogrendszere. Míg az USA-ban a common law, vagy angolszász jog érvényesül, mely a bírói joggyakorlatot preferálja, precedenseket teremtve, ami lehetővé teszi azt, hogy egy államon belül is másképp értelmezzék az írott jogot, vagy egy adott ügy kapcsán új értelmezést nyerjen. [1]
Az európai adatvédelmet háromgenerációsnak tekinti a szakirodalom, melynek kezdetben a polgár állammal szembeni kiszolgáltatottságának csökkentése volt az elsődleges célja, ami megteremtette a polgárok tájékoztatáshoz való jogát. A második generációs adatvédelemnél már megjelentek az információs

[33] Óbudai Egyetem Biztonságtudományi DoktoriIskola Ph.D hallgató

önrendelkezési jog csírái. Míg a harmadik generációs adatvédelem kialakulását a technika és az üzleti világ fejlődése eredményezte. A polgárosodás során a személyes adatok védelme mellett fokozatosan került előtérbe az állam átláthatóságának igénye, a közérdekű adatok megismeréséhez és terjesztéséhez való jog és az információszabadság, mely magával hozta az állami és egyéb közhatalmi szervek működésének és a közpénz-felhasználás átláthatóságának az igényét is. A felsoroltak támogatták az állam demokratikus működését. [2]
Az Európai Unió adatvédelmét az OECD (Gazdasági Együttműködés és Fejlesztési Szervezet) 1980-ban hatályba lépett nemzetközi megegyezésen alapuló adatvédelmi jogi irányelve alapozza meg, mely középpontjában a személyes adatok magas védelme mellett a gazdasági kapcsolatok akadálymentes működése állt.
Az OECD által megalkotott alapelvek hatottak az Európa Tanács 1981-ben elfogadott "Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során" című egyezményre. [3]
2001-ben létrehozták az Európai Adatvédelmi Biztos tisztséget, akinek a feladata, hogy biztosítsa a személyes adatok feldolgozása során, hogy az összes uniós intézmény és szerv tekintettel legyen a polgárok magánéletének tiszteletben tartásához való jogára. [4]
Ezzel szemben az USA-ban az egyének joga az adataik védelméhez gyengébb, mint Európában. Annak ellenére, hogy 1890-ben megjelent egy amerikai tanulmány Samuel Warren és Louis Brandeis jogászoktól, mely elsőként fogalmazza meg, hogy a technika fejlődése és a nyilvánosság új megvalósulása már sérti a magánszférát. Ez szükségessé teszi egy új típusú védelmi rendszer megalkotását, ami az információs önrendelkezési jog, amit a jó hírnévhez való jogon keresztül közelít meg. Ez az 1970-es évekre forrott ki, amikor, mint alapjogra hivatkozva alakították ki a polgárok védelmét a nagy állami nyilvántartásokkal szemben. A továbbiakban a folyamat legfontosabb mérföldköveit fogom bemutatni Molnár András tanulmánya alapján. [7] [8]
Az 1928-as Olmstead v. United States-ügy esetében a legfelsőbb bíróság többségi döntéssel megállapította, hogy a bírói végzés nélküli telefonlehallgatások nem sértenek alkotmányos alapjogot, ugyanis az csak a fizikálisan csak a házon belül értelmezi a magánszféra védelmét. Ennek az ítéletnek hatására fogalmazta meg ellenpólusként szintén Louis Brandeis a " the right to be let alone"-t, amit a békén hagyás jogaként lehet értelmezni.
A "right of privacy" is viszonylag későn az 1960-as években került az alkotmányos alapjogi fogalmak közé, mint tételes gyűjtőfogalom, de szó szerinti alkalmazásban nem szerepel az USA alkotmányában.

William Prosser jogászprofesszor a magánszférához való jogot kártérítési jogrendszerbe helyezi el, ahol a magánszférához való jog sérelmei közt szerepel a magánjellegű tények nyilvános közzététele, mely az érintettek számára hátrányos helyzetet eredményez, a valóságtartalomtól függetlenül. Külön kategóriaként jelenik meg a nyilvánosság számára hamis színben való megjelenítés. Szintén a magánszférához tartozó jog elemeként jelent meg a képmás, név és egyéb azonosítók birtoklása. Később Gary Bostwick a védett érdekek közé sorolta, mint biztonságos fűződő érdeket, miszerint a külső felek csak egy bizonyos védett zónáig férhetnek hozzá ez egyénnel kapcsolatos információkhoz. 1977-es Legfelsőbb Bírósági ítélet Whalen v. Roe ügy kapcsán fogalmazta meg, hogy a magánszférával kapcsolatos ügyek által érintett érdekek több különálló érdekből tevődnek össze, melyek közé tartozik az egyénnel kapcsolatos információk és azok rejtve maradásának érdeke. [9]
David Solove 2006-os tanulmányában a jogosulatlan információgyűjtést alapjogsértésnek tekinti, ugyanúgy ide sorolja a jogszerűen megszerzett információval való visszaélést és az információ megszerzés módjától függetlenül annak nagy nyilvánosság felé publikálását is.
Összegezve az USA-ban nem érvényesül egységes adatvédelmi jog, ugyanis adott a lehetőség arra, hogy tagállamonként eltérően értelmezzék. Annak ellenére, hogy egyes bíróságok az adatvédelmet alapjognak ítélték, nincs egységes hatósági felügyelete. Másik gyenge pontja, hogy a "Privacy Act" (szövetségi szintű adatvédelmi törvény) hatálya alá csak az amerikai állampolgársággal, vagy az amerikai tartózkodási engedéllyel rendelkező személyek tartoznak.

2. Az Európai Unió és az USA kapcsolata

Az adatvédelem és az információs önrendelkezési jog az információs társadalmak kialakulásával egyre kevésbé tud érvényesülni. A társadalmi, gazdasági, technikai különbségek miatt a fejletlenebb országok adataikat tekintve sokszor kiszolgáltatottá válnak a náluk fejlettebb országokkal szemben, melyek a technológiai szakadékot kihasználva nem bejelentett adatgyűjtést, adatbányászatot végeznek. Az ilyen jellegű kiszolgáltatottság csökkentésének egyik módja, az adatgyűjtés, adatkezelés legalizálása országok közötti kölcsönös megegyezéssel, garanciák beiktatásával. Ennek a felfogásnak tesz eleget a gazdasági kapcsolatokat segítő OECED (Gazdasági Együttműködési és Fejlesztési Szervezet) és az Európai Unió jogharmonizációja is.
Az USA-ba történő adattovábbítás megkönnyítésére hozták létre a "Safe Harbour"-t Harmadik országba történő adattovábbítás fő követelménye, hogy az

adatfeldolgozás során biztosítva legyen a személyes adatok megfelelő szintű védelme. Az Európai Unió Bizottsága szerint az USA-ban akkor tekinthető a védelem megfelelő szintűnek, ha a címzett amerikai vállalat szerepel a Safe Harbour listán, vagy ha utas-nyilvántartási adatokat továbbítanak az Egyesült Államok Vámügyi és Határvédelmi Irodájának.
A Safe Harbour listán azok a vállalatok szerepelnek, melyek vállalták, hogy teljesítik az USA kormánya által deklarált, a személyes adatok védelmét szabályozó Safe Harbour adatvédelmi elveket.
Mindezek jogalapját a Bizottság 2000. július 26-i 2000/520/EK határozata a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott (biztonságos kikötő adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről szóló) dokumentum adja. Ebben a határozatban szerepelnek azok az adatvédelmi elvek is, amelyeknek az USA-ban jegyzett vállalatoknak meg kell felelniük. [10]
A Stockholmi-program keretében az Európa Parlament felkéri az Európai Bizottságot, hogy az információcserével, azonfelül a magánélet és a személyes adatok védelmével foglalkozó Európai Unió–USA magas szintű kapcsolattartó csoport által készített eredményekre építve készítsen ajánlást az USA-val kötendő, bűnüldözést célzó adatvédelmi, illetve adott esetben adatcsere-megállapodással kapcsolatos tárgyalásokra. A 29. cikk szerinti adatvédelmi munkacsoport Jacob Kohnstamm elnökletével megállapította, hogy az utas-nyilvántartási adatállomány (továbbiakban: PNR) olyan nagymennyiségű személyes adatokat gyűjt az összes EU-ból utazó polgárokról, mely túllépik a szükségesség és az arányosság elvét. A súlyos bűncselekmények és a terrorizmus elleni védekezés nem indokolja a tömeges utas nyomonkövetést és megfigyelést. Az ehhez hasonló rendőrségi módszerek az Európai Unió tagállamaiban kizárólag alkotmányos keretek között, különleges esetekben hajtható végre. A munkacsoport megállapította, hogy még nem látott olyan statisztikát, amely a PNR-rendszer segítségével elfogott személyek számát összeveti a nyilvántartott törvénytisztelő utasok számával és ezzel a szükségességét alátámasztja. Ezért véleményük szerint szűkítni kellene a PNR-rendszerben kezelt adatok körét. Az európai adatvédelmi biztossal egyetértve a munkacsoport nem tartja elfogadhatónak, hogy a Belbiztonsági Minisztérium különleges adatokat tart nyilván, még akkor is ha ezt rejtett adatként kezeli. Továbbá aránytalannak tartja az adatok maximalizált 15 éves megőrzését, ugyanis az Európai Unió Alapjogi Chartája szerint az adatokat a felhasználást követően, vagy legfeljebb hat hónap után anonimizálni, vagy törölni kell.

Az európai adatvédelmi biztos támogatja, hogy a PNR-adatokhoz való valamennyi hozzáférést, adatfeldolgozását kötelezően naplózzák és dokumentálják, mivel ezáltal ellenőrizhetővé válik, hogy a Belbiztonsági Minisztérium megfelelően használja-e fel az adatokat. [11] [12]
A transzatlanti partnerség fontos szerepet játszik az Európai Unió külpolitikájában, mely célja 2015-ig létrehozni a transzatlanti piacot. A transzatlanti partnerség során az Európai Unió elvárja, hogy az általa képviselt értékeket a partner is elfogadja. Ilyenek a demokrácia, az emberi jogok és a jogállamiság, a fenntartható gazdaság és a fenntartható fejlődés. Ezen értékeknek az olyan globális kockázatok elleni védekezés esetén is érvényesülni kell, mint a nemzetközi terrorizmus. Annak ellenére, hogy az USA és az Európai Unió tekinthető a világ legnagyobb kétoldalú kereskedelmi partnerének a termékek és a szolgáltatások terén, mely gazdasági függőséget is okoz, mégis az USA tettei - melyek abbahagyására az Európai Parlament több alkalommal is felszólította az USA Kormányát - sok ízben ellentmondanak az Európai Unió által deklarált értékeknek pl.: USA egyes tagállamaiban elfogadott a halálbüntetés alkalmazása, Guantánamo-öbölben lévő fogolytábor fenntartása, bizonyos európai uniós tagállamokkal szembeni egyoldalú vízumkötelezettség alkalmazása. A terrorizmus gyanújába keveredett személyeket a beigazolódott ártatlanságukat követően se törlik a nyilvántartásaikból, továbbá a névrokonokról is nyilvántartást vezetnek és nem utolsó sorban a amerikai Nemzetbiztonsági Ügynökség (NSA) titkos információ gyűjtési gyakorlata. [13]

Összegzés

A két hatalom között a jogértelmezési ellentét túl mutat a történelmi gyökereken. Annak ellenére, hogy az USA is több államból tevődik össze, külpolitikája nem tekinti az Európai Uniót egységes egészként és eltérő bánásmóddal bír a tagállamokkal szemben.
Az USA emberi jogokkal összefüggő adatvédelmi és információs önrendelkezési jog értelmezése is erősen eltér az Európai Unió által deklaráltaktól. A fentiek hosszútávon veszélyeztethetik a transzatlanti partnerség megvalósulását, vagy amennyiben a fennálló feltételekkel kötik meg partnerséget az Európai Unió, mint alárendelt fél fog megjelenni a gazdasági kapcsolatokban.

Felhasznált irodalom:

[1] Gönczi Katalin - Dr. Horváth Pál - Stipta István - Zlinszky János: Egyetemes jogtörténet (Nemzedékek Tudása Tankönyvkiadó, 2002.,ISBN: 9789631945720)

[2]Jóri András: Adatvédelmi kézikönyv, OSIRIS KIADÓ KFT., 2005.

[3]Gazdasági Együttműködési és Fejlesztési Szervezet (OECD), általános tájékoztató (Letöltve:http://oecd.kormany.hu/az-oecd-rol, 2013.11.09

[4]Az Európai és a Tanács 95/46/EK irányelve (1995. október 24.) (Letöltve:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:hu:HTML, 2013.11.09.)

[5]Az Európai Adatvédelmi Biztos, általános tájékoztató(Letöltve: http://europa.eu/about-eu/institutions-bodies/edps/index_hu.htm, 2013.11.09.)

[6]Adatvédelmi Biztos honlapja, általános tájékoztató (Letöltve: http://abi.atlatszo.hu/index201.php?menu=usa, 2013. 11.26.)

[7]Molnár András: A magánszférához való jog az Amerikai Legfelsőbb Bíróság joggyakorlatában (Letöltve: http://dieip.hu/wp-content/uploads/2011-2-11.pdf, 2013. 11. 25.)

[8]Győrfi Tamás: Az amerikai alkotmányjog szabadság-fogalma (Letöltve: http://jesz.ajk.elte.hu/gyorfi4.html, 2013.11.25.)

[9]Dr. Rajnai Zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23., ZMNE, Budapest, 2010

[10]Adatvédelmi Biztos honlapja, általános tájékoztató (Letöltve: http://abi.atlatszo.hu/index201.php?menu=safeharbour, 2013. 11.26.)

[11]A stockholmi program – A polgárokat szolgáló és védő, nyitott és biztonságos Európa 2010/C 115/01 (Letöltve http://eur-lex.europa.eu/Notice.do?mode=dbl&ihmlang=en&lng1=en,hu&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=513011:cs, 2013.12.01.)

[12]29. cikk szerinti adatvédelmi munkacsoport, 00664/11/HU WP 181, 10/2011 sz. vélemény „az utas-nyilvántartási adatállomány (PNR) felhasználásáról a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntető eljárás alá vonása érdekében” című, európai parlamenti és tanácsi irányelvre irányuló javaslatról, 2011. április 5. (Letöltve: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_hu.pdf , 2013.12.01.)

[13]Az Európai Unió Hivatalos lapja: P6_TA(2006)0238 EU–USA transzatlanti partnerségi megállapodás, C298 E/226, 2006. 12.18.(Letöltve: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:298E:0235:0235:HU:PDF, 2013.11.26.)

Szabó Anna Barbara: Adatvédelem fejlődése (jogi megközelítésből)

Absztrakt:
A személyes adatok kezelése és védelme szorosan összekapcsolódik az állami struktúrák kialakulásával, első sorban harcászati és állam igazgatási okok miatt. Az államformák és a technika fejlődésével a gyűjtött adatok köre bővült, célja is megváltozott. Az információs társadalmak kialakulásával az információval bíró adatok felértékelődtek, egy sajátos függőség alakult ki, ahol az adat hatalmi tényezővé vált. A kezelt összetett adatbázisok túl mutatnak az egyén közteherviselésével összefüggő és ahhoz szükséges adatokon, eljutottak egészen a magánszféráig, így szükségessé vált a szabályzása.

Abstract
The management and protection of personal data is closely linked to the development of state structures, mainly because of tactical and administrative reasons. Because of the development of technology and changes in governmental forms the range of collected data expanded and the purpose changed. With the emergence of information societies the collected informative data has been appreciated, and a dependence has been established where data has become a power factor. The currently managed database is too complex, integrated with public burdens and even concerns more, reaching the private sector, that is why it is essential to control it.

1. Adatvédelem generációi

Jelenleg a szakirodalom az európai az adatvédelmet három generációsnak tekintheti.
Az első generációs adatvédelem célja a polgár állammal szembeni kiszolgáltatottságának csökkentését célozta meg. A szabályozások jellemzően technikai jellegűek voltak, amelyek az adatkezelés átláthatóságát igyekezetett megteremteni. Ebből kifolyólag az állampolgárok már rendelkeztek adataik kezelésével kapcsolatban jogokkal, mint például a tájékoztatás és a helyesbítés.
A második generációs adatvédelmet a német alkotmánybíróság 1983-as ítéletétől lehet eredeztetni, mely az információs önrendelkezési jogot az általános személyiségi jogból vezeti le, ebből kifolyólag minden polgárt megillet. Az érintett

alapesetben magánéletével összefüggő adatai terén már döntési joggal is bír. Az ekkor keletkezett szabályozások absztraktnak és technika-semlegesen tekinthetőek. A harmadik generációs adatvédelem kialakulását a technika és az üzleti világ fejlődése eredményezte. A korábbi szabályozás már nem voltak elég polgárok magánszférájának megvédésére. A megoldás az ágazat-specifikus szabályzás és egy a technika fejlődésével állandó párhuzamos modernizált általános adatvédelmi szabályzat megfogalmazása lett. [1]
A polgárosodással személyes adatok védelme mellett fokozatosan jelnet meg az, állam átláthatóságának igénye, a közérdekű adatok megismeréséhez és terjesztéséhez való jog, az információszabadság. Az állampolgárok betekintést akartak nyerni az állami és egyéb közhatalmi szervek működésébe és a közpénzek felhasználásába.
A közérdekű adatok megjelenése segíti a népi kontroll által demokratikus működést, serkenti az államigazgatási szervek hatékonyságát, az állampolgárok közügyekben való részvételét, a korrupció és állami visszaélések elleni fellépést, mely a véleménynyilvánítás jogát is eredményezte.

2. Az adatvédelem nemzetközi szabályozása

Az adatvédelmi szabályozások összehangolásának fő motivációja, hogy az országonként különböző adatvédelmi szabályok és adatfeldolgozások ne akadályozzák a nemzetközi gazdasági kapcsolatok fejlődését.
Az OECD (Gazdasági Együttműködés és Fejlesztési Szervezet) 1980-ban olyan nemzetközi megegyezésen alapuló adatvédelmi jogi irányelvet alkotott, mely személyes adatok magas védelmét és a gazdasági kapcsolatok gördülékeny működését egyaránt lehetővé teszi és hatálybalépése óta kiindulási alapja a személyes adtok védelmét biztosító garanciáknak.
Az OECD által megfogalmazott alapelvek hatással voltak az "Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során" című egyezményre, melyet az Európa Tanács 1981-ben elfogadott. [1][2]
1995 októberében lépett hatályba az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, mely az adatfeldolgozás szempontjából polgárok személyes adatainak védelme mellett az adatok szabad áramlását is igyekezett megteremteni a tagállamok között. Továbbra is a gazdasági szempontok voltak fontosak, így a kereskedelmi és gazdasági együttműködéssel összefüggő személyes adatok kezelésének formáit szabályozta. A tagállamok jogharmonizációs

kötelezettsége miatt az irányelv adatvédelmi rendelkezéseit bele kellett venni a nemzeti joganyagba. [1] [3]
A harmonizáció során főbb témaköröknek számított az adatvédelmi jog alapvető definiálása, adatvédelmi alapelvek érvényesítése, harmadik országokba irányuló adattovábbítás követelményei, a különleges adatok védelmére vonatkozó speciális szabályok megalkotása, az érintettek jogainak biztosítása, jogellenes adatkezeléssel szembeni szankció felállítása.
2001-ben létrejött az Európai Adatvédelmi Biztos (EDPS) tisztsége. Feladata, hogy biztosítsa a személyes adatok feldolgozása során azt, hogy az összes uniós intézmény és szerv tekintettel legyen a polgárok magánéletének tiszteletben tartásához való jogára. [4]

3. Adatvédelem szabályozása Magyarországon

A legfontosabb adatvédelmi szabály 2011. április 25-ig az Alkotmány volt, mely a magánszféra védelme felöl közelítette meg az adatvédelmet. Jelenleg Magyarország Alaptörvénye a magánszféra védelme mellett kimondja, hogy mindenkinek joga van személyes adatai védelméhez és a közérdekű adatok megismeréséhez, terjesztéséhez. [5]
Az első adatvédelmi törvény az 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvény volt, mely a fő vonalait tekintve megfelelt az Európai Unió előírásainak, ugyanakkor részletszabályait tekintve szükséges volt módosítani az uniós csatlakozás során. A 2011-es évben az Országgyűlés új adatvédelmi törvényt fogadott el, a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról című törvényt (továbbiakban: Iötv.), mely már nevében is az egyén információs önrendelkezési jogát igyekezett kihangsúlyozni. Így a szabályozás nem terjed ki a jogi személyek és az elhunytak adatainak a védelmére. [6] [7]
A törvény az alábbi adatfajtákat különbözteti meg: [7]
Személyes adat: azon adatok köre, melyek az érintettel kapcsolatba hozhatóak és az adatból levonható következtetés, mindaddig, amíg az adat és az érintett között a kapcsolat helyreállítható. Pl.: név, azonosító jel, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző információ. A személyes adat speciális fajtája a különleges adat.
Különleges adat: a különleges adat két csoportra bontható:
Faji eredetre, a nemzetiséghez való tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat.

Egészségi állapotra, kóros szenvedélyre vonatkozó személyes adat, azonfelül a bűnügyi személyes adat.

Bűnügyi személyes adat olyan adat, mely büntetőeljárás alatt vagy azt megelőzően a bűncselekménnyel vagy azzal összefüggésben, annak lefolytatására. Ide tartoznak azok az adatok is, melyek a bűncselekmények felderítésére jogosult szerveknél és a büntetés-végrehajtás szervezeténél keletkezett és az érintettel kapcsolatba hozható, továbbá a büntetett előéletre vonatkozó személyes adatok is.

Közérdekű adat: azon adatok, melyek állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett. Azon információk, vagy ismeretek, melyek nem minősülnek személyes adatnak, a rögzítésének és kezelésének módjától függetlenül. Azon adatok, melyek hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésre, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkoznak.

Közérdekből nyilvános adat: azon adatok, melyeket nyilvánosságra hozatalát, megismerhetőségét, hozzáférhetővé tételét törvény közérdekből elrendeli és a közérdekű adat fogalma alá nem sorolható be.

A törvény különbséget tesz az adatkezelés és adatfeldolgozás között.

Adatkezelés: az adatokon végzett művelet vagy a műveletek összessége, függetlenül az eljárástól. Tehát a gyűjtés, felvétel, rögzítés, rendszerezés, tárolás, megváltoztatás, felhasználás, lekérdezés, továbbítás, nyilvánosságra hozatal, összehangolás vagy összekapcsolás, zárolás, törlés és megsemmisítés. Ide tartozik az adatok további felhasználásának megakadályozása, ugyanakkor a fénykép-, hang- vagy képfelvétel készítése és a személy azonosítására alkalmas fizikai jellemzők rögzítése is.

Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok, függetlenül az alkalmazott módszertől, eszköztől és a helyétől, feltétele, hogy a technikai feladatokat az adatokon végezzék.

A fentiekből következik, hogy az adatkezelő az a személy, aki az adatkezelésre vonatkozó érdemi döntéseket hozza és meghatározza a kezelés célját. Ezzel szemben az adatfeldolgozó az, aki az adatkezelővel kötött írásbeli szerződése alapján, elvégzi az adatokon a technikai műveleteket. Személyes adat csak akkor kezelhető, ha ahhoz az érintett hozzájárult, vagy azt törvény vagy helyi önkormányzati rendelet előírta. Az érintett hozzájárulásának előzetes tájékoztatáson kell alapulnia, egyértelműnek kell lennie és önkéntesnek. Különleges adatkezeléshez a cselekvőképes érintett írásbeli hozzájárulása kell, 16

év alatti személy esetén jognyilatkozata érvényességéhez a törvényes képviselő beleegyezés, vagy utólagos jóváhagyása is kell.
Az érintett hozzájárulása vélelmezésen alapul szükséghelyzetben, érintett kérelmére indított eljárás során és közszereplés esetén. Az Iötv. adatkezelés jogalapjának tekinti azt is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, viszont az adatkezelése az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából, vagy az adatkezelő illetve harmadik személy jogos érdekének érvényesítéséhez szükséges. Amennyiben az adatkezelő jogi kötelezettségnek teljesítése, vagy jogos érdekének érvényesítése érdekében szükséges a kezelt adat, hiába vonja vissza az érintett az adatkezeléshez való hozzájárulását, az adat nem kerül törléshez.
A kötelező adatkezelés során a jogalkotó közérdeken alapuló célból törvényben szabályozza az adatkezelést, mely során az érintett adatit illető rendelkezési joga korlátozás alá kerül. Ebben az esetben az adatkezelés célját, feltételeit, a kezelendő adatok fajtáit és megismerhetőségét, az adatkezelés időtartamát, az adatkezelőt a törvény, vagy önkormányzati rendelet határozza meg.
Az adatkezelése során figyelemmel kell lennie az adatkezelőnek az adatvédelem alapelveire. Az alapelvek egymással összefüggésben vannak és az adatkezelés során egyaránt érvényesülniük kell. [7]
Tisztességes adatkezelés elve: az adatkezelésnek meg kell felelnie eredetileg rögzített céljával, az adatok felvételének törvényesen és tisztességesen kell történnie.
Célhoz kötöttség elve: az adatkezelést mindig és minden szakaszában jogszerűen és pontosan meghatározott célból kell végezni, annak megszűnésével az adatkezelést meg kell szüntetni. Az adatkezelés céljáról az érintettet tájékoztatni kell, úgy, hogy tudja mérlegelni, milyen hatással van rá az adatainak kiadása, illetve, hogy jogorvoslattal élhessen az előzetesen ismertetett céltól eltérő adatkezelés esetén.
Adatminimalizálás elve: szorosan összefügg a célhoz kötöttség elvével, ugyanis az alapelv szerint az adatkezelés a csak a cél eléréshez szükséges ideig és mértékig mehet végbe.
Személyes adatok minőségének elve: eszerint az adatkezelés ideje alatt biztosítani kell az adatok pontosságát, teljességét és naprakészségét. Ide tartozik az is, hogy az érintett csak a szükséges ideig lehessen beazonosítani, ezt a tárolás során is figyelembe kell venni.

Az adatbiztonság érvényesüléséhez a rendelkezésre álló adatokat minden lehetséges fenyegetéstől meg kell védeni: így az adatok sérthetetlenségét

(integrity), a rendelkezésre állását (availability) és bizalmasságát (confidentiality) egyszerre. Az Országgyűlés 1995. nyarán hozta létre az Adatvédelmi Biztos Hivatalát, mely egészen 2012. január 1-ig működött. Helyét az Iötv. hatálybalépést követően a Nemzeti Adatvédelmi és Információszabadság Hatóság vette át. Érdemleges különbség a két szerv között, hogy az utóbbi jogellenes adatkezelés során hatóságként léphet fel, határozatában bírságot is szabhat ki, míg elődje csak ajánlást fogalmazhatott meg, jogellenes adatkezelés esetén megszüntetésére irányuló felszólítását nem követte szankció.

Összegzés

Megállapítható, hogy az adatvédelem fejlődése a társadalmi formák fejlődésével párhuzamosan alakult. Az államformák kialakulásával egyre nagyobb mennyiségű adatok kezelése vált szükségessé, a polgárosodással viszont az érintettek jogai is megjelentek a személyes adataik kezelésével összefüggően.
Magyarországon az Európai Unós csatlakozás előtt is fejlett volt az személyes adatok védelmének szabályozása, melyben nagy szerepet töltött be az OECD által megfogalmazott alapelvek felhasználása. Az adat és információ védelem fejlődésében jelentős előrelépésnek számit, hogy a Nemzeti Adatvédelmi és Információszabadság Hatóság létrehozása.

Felhasznált irodalom

[1]. Jóri András: Adatvédelmi kézikönyv, OSIRIS KIADÓ KFT., 2005.
[2]. Gazdasági Együttműködési és Fejlesztési Szervezet (OECD), általános tájékoztató (Letöltve:http://oecd.kormany.hu/az-oecd-rol, 2013.11.09.)
[3]. Az Európai és a Tanács 95/46/EK irányelve (1995. október 24.) (Letöltve:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:hu:HTML,2013.11.09.)
[4]. Az Európai Adatvédelmi Biztos, általános tájékoztató (Letöltve: http://europa.eu/about-eu/institutions-bodies/edps/index_hu.htm, 2013.11.09.)
[5]. Magyarország Alaptörvénye (Letöltve: http://njt.hu/cgi_bin/njt_doc.cgi?docid=140968.248458, 2013.11.09.)
[6]. 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (Letöltve: http://njt.hu/cgi_bin/njt_doc.cgi?docid=17324.26713, 2013.11.09.)

[7]. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
(Letöltve: http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.245254, 2013.11.09.)
[8] Dr. Rajnai Zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23., ZMNE, Budapest, 2013

Puskás Béla: Az informatikai rendszerek és a jogi környezet változásai

Absztrakt
"A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága."[34]
A jogi környezet kialakítása egy fontos IT környezeti feltétel megteremtése volt, hogy szabályozott és biztonságos keretek közt működhessenek az informatikai rendszerek. A megtett lépéseket leginkább a KRESZ[35] *kialakulásának történetével lehetne összehasonlítani. A technika fejlődik, majd elér egy bizonyos szintre, ahonnan már szabályozni kell a működést. A szabályozás regionális szinten történik meg, majd összehangolják ezeket nemzetközi szinten is. A digitális bennszülöttek korában, akik már akkor tudják használni a technikai eszközöket, amikor még beszélni sem tudnak fontos és halaszthatatlan lépés volt a szabályzás. A Z generáció legtöbb idejét a közösségi oldalakon tölti, az életét úgy szervezi, hogy elképzelhetetlen lenne az Internet nélkül.*

Abstract
This article shows the management of classified data in Hungary.

1. Minősített adatok védelme

2010 év egyfajta mérföldkő volt Magyarországon az információbiztonság terén, ezen belül is kiemelt figyelmet kapott az informatikai biztonság. Míg korábban leginkább a szabványok, szokások segítették a CIO[36]-kat a informatikai rendszerek biztonságosabb üzemeltetésében, mára szélesebb lehetőségből választhatnak, illetve sok mindennek kell megfelelni ezen a téren.
2009. XII. 29-n került kihirdetésre a minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.). A megalkotására és minél hamarabbi bevezetésére több dolog miatt is szükség volt.

[34] 2013. évi L. törvény
[35] KRESZ- Közúti Rendelkezések Egységes Szabályozása
[36] CIO - Chief Information Officer

1996-ban Magyarország aláírta a Nyugat-európai Unióval (a továbbiakban: NYEU) a Biztonsági Megállapodást, melynek értelmében kötelezettséget váltunk arra, hogy a megkapott védendő információkat az előírások szerint kezeljük és tároljuk.
A NATO Biztonsági szabályzata (NATO CM (55) 15). [1] A NATO csatlakozásunk egyik kitétele volt, hogy elfogadjuk az Információ Biztonságról szóló Megállapodást. Ebben rögzítették, hogy létre kell hozni egy nemzeti biztonsági hatóságot, amely helyileg felügyeli a biztonsági feltételek meglétét az adott országban.
A Nemzeti Biztonsági Felügyeletről (a továbbiakban: NBF) szóló 1998. évi LXXXV. törvényt az Országgyűlés 1998. december 22-i ülésnapján fogadta el. A NBF akkor még kizárólag a NATO és NYEU Biztonsági Szabályzatában előírt követelmények érvényesítéséért volt a felelős, és a polgári nemzetbiztonsági szolgálatokat irányító miniszter irányítása alatt állt. 2003-ban az EU-hoz való csatlakozásunkkor a feladatköre kibővült az Európai Unió Tanácsa és az Európai Unió Bizottsága, valamint az EURATOM Biztonsági Szabályzataiban leírtak érvényesítésével.
A 179/2003. Kormány rendeletben a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályai már az elektronikus adatkezelésre is kitértek.
2073/2004 Kormány határozat[37] felhívja a figyelmet az informatikai területen való elmaradásunkra, illetve kockázati tényezőként említi az esetleges negatív következményeket. A védendő nemzeti információkkal kapcsolatban még az utoljára 2007-ben módosított 1998. évi LXXXV. törvény sem adott felhatalmazást az NBF-nek. 2009-ben a Mavtv. hatálytalanította a LXXXV-as törvényt, valamint már a nemzeti minősített adatok felügyeletet is a szervezet kezébe adta. A hazai és a szövetséges adatokat ugyanolyan szintű védelemmel kell ellátni. Ezzel biztosítható az elektronikus adatok mozgatása a rendszerek közt. A megfeleltetéssel egy magasabb szintre került a nemzeti adatok védelme is. A szigorítás mellett fontos előrelépés volt az, hogy az informatikai rendszerek üzemeltetéséről, védelméről érdemben foglalkozik a törvény és a hozzá kapcsolódó rendeletek. A rendeletek hierarchikusan a törvények alatt helyezkednek el, rendeletalkotásra csak törvényi felhatalmazás alapján kerülhet sor. A Mavtv. megjelenését követően 90/2010. Kormány rendelet a Nemzeti Biztonsági Felügyelet működését, valamint a minősített adat kezelésének rendjét szabályozza. Még ugyancsak 2010-ben elfogadták a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. Kormány rendeletet. A Mavtv. a minősítési szint meghatározásához az okozott kár mértékét veszik figyelembe. Így létezik

[37] a Magyar Köztársaság nemzeti biztonsági stratégiájáról

1. **„Szigorúan titkos!"**, amennyiben rendkívül súlyos kárnak minősül. „Szigorúan titkos minősítési szint alkalmazása indokolt, ha az adat érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele közvetlenül és tartósan sérti vagy veszélyezteti Magyarország szuverenitását, területi integritását, törvényes rendjét, belső stabilitását. Visszafordíthatatlanul jelentős károkat okoz az ország honvédelmi, nemzetbiztonsági, bűnüldözési, igazságszolgáltatási, központi pénzügyi és gazdasági érdekeiben, külügyi és nemzetközi kapcsolataiban, a szövetséges tagállamokkal közös biztonsági érdekeiben. Rendkívül súlyosnak minősülhet a kár akkor is, ha annak elkerülhetetlen enyhítése nagyszámú emberi élet közvetlen veszélyeztetésével, vagy az ország gazdasági helyzetének egészére hátrányosan kiható ellenintézkedésekkel érhető el." [2]
2. **„Titkos!",** ami súlyos kárnak minősül. „Titkos minősítési szint alkalmazása indokolt, ha az adat érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele által az 1. pontban okozott sérelem nem küszöbölhető ki, de enyhíthető, továbbá, ha ellehetetleníti vagy lényegesen akadályozza az állami vagy közfeladatot ellátó szerv rendeltetésszerű működését és ezáltal közvetlenül Magyarország törvényben meghatározott érdekeit sérti, az állampolgárok biztonságának és alkotmányos jogainak komoly sérelmével jár, közvetlen életveszélyt okoz, jelentősen hátráltatja a honvédelmi és nemzetbiztonsági tevékenység folyamatos hatékonyságát, feszültséget okoz Magyarország más országokkal fennálló kapcsolataiban, a szövetséges tagállamokkal közös biztonsági érdekeiben, Magyarország pénzügyi és gazdasági érdekeinek sérelmével számottevő vagyoni kárt okoz." [3]
3. **„Bizalmas!",** ami súlyos kárnak minősül. „Bizalmas minősítési szint alkalmazása indokolt, ha az adat érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele okozta érdeksérelem vagy veszélyeztetés ellenintézkedésekkel lényegesen enyhíthető, és az nem jár jelentős anyagi, pénzügyi ráfordításokkal. Továbbá, ha az állam érdekérvényesítő képességeit hátráltatja, vagy jelentősen zavarja, a diplomáciai kapcsolatok tényleges sérelmét eredményezi, aminek következménye hivatalos tiltakozás vagy enyhébb szankció lehet, sérti az állampolgárok biztonságát és alkotmányos jogait, jelentősen sérti a nemzetgazdasági szempontból kiemelt jelentőségű gazdasági szervezet

működését, hátráltatja a honvédelem és a nemzetbiztonsági tevékenység, illetve a szövetséges tagállamokkal közös biztonsági érdekek védelmének hatékonyságát, gátolja valamely legalább öt évi szabadságvesztéssel büntetendő bűncselekmény felderítését vagy elősegíti valamely ilyen bűncselekmény elkövetését, megzavarja az állami vagy közfeladatot ellátó szerv működési rendjét, feladat- és hatáskörének gyakorlását és ezáltal közvetve Magyarország törvényben meghatározott érdekeit sérti." [4]

4. **„Korlátozott terjesztésű!”,** ami hátrányosan érinti az állam érdekeit. „Korlátozott terjesztésű minősítési szint alkalmazása indokolt, ha az adat érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele megzavarja az állami vagy közfeladatot ellátó szerv működési rendjét, feladat- és hatáskörének gyakorlását és ezáltal közvetve Magyarország törvényben meghatározott érdekeit hátrányosan érinti, a hátrány azonban az elhárítására tett intézkedésekkel lényegesen enyhíthető vagy kiküszöbölhető. Az államnak az 1-3. pontba nem tartozó pénzügyi veszteséget okoz, továbbá, ha az állampolgárok vagy a gazdálkodó szervezetek részére jogtalan nyereséget vagy előnyszerzést tesz lehetővé." [5]

A rendszerekre vonatkozó fizikai, elektronikai, adminisztratív biztonsági követelményeket a 90/2010. és a 161/2010. Kormányrendeletekben határozzák meg. A jogalkotók a hatósági jogkört az NBF-nek címezték a minősített rendszerekkel kapcsolatban. A rendeletekben konkrét munkaköröket és azok feladatrendszerét is meghatározzák. Pontos hierarchiai felépítés szükséges egy minősített adatot felhasználó szervezetnél. Azonban sajnos több esetben ezeket a munkákat a munkaadók, mint a tényleges beosztás mellett elvégzendő egyéb feladatként értelmezték, értelmezik. Amennyiben ezeket a feladatokat komolyan, a törvényalkotók által elgondolt minőségben látják el, akkor egy teljes napi elfoglaltságot jelentene a munkavállalónak. Valószínű, hogy a döntéshozók gondolkodásmódjában is komoly változásoknak kell bekövetkezni, mert a munkakörnyezet, a mindennapi élet sokszor gyorsabban változik, mint a generációváltás. Szintén szigorú feltételeknek kell megfelelni a fizikai kiépítés esetében is, ahol legfontosabb kategóriák a biztonsági zóna és az adminisztratív terület. A biztonsági zónán belül két osztály létezik az I. osztályú biztonsági terület, ahol a minősített adatok nyílt tárolása is lehetséges, valamint a II. osztályú biztonsági terület, ahol a minősített adatok csak zártan tárolhatók. A tárolás mellett természetesen a felhasználás mindkét esetben megengedett. A szervertermeket, -

amennyiben minősített adatokat felhasználó rendszerek kiszolgálására hoztak létre, tipikusan az I. osztályú biztonsági területként kell létrehozni. A munkaállomások, amelyeken minősített adatokat dolgoznak fel, már lehet mindkét helyszínen használni, amennyiben az adatok tárolására alkalmas elemeit a munkavégzést követően elzárjuk megfelelő védelemmel ellátatott helyre.
Külön kitér a jogszabály a reagáló erőkre, az elektronikus jelzőrendszerre, beléptető rendszerekre, ajtókra, tárolókra, zárakra, falakra, stb. A felsorolásból is látható, hogy egy meglévő szervertermet lehetetlen, vagy komoly anyagi ráfordítással lehet a megfelelő szintre hozni. Az újonnan épülő helyiségeket ezeknek megfelelően kell létrehozni, amelyre komoly figyelmet kell fordítani már a tervezések megkezdésekor. A tervezéseknél számolni kell a várható költségekkel, és a szükséges időtényezőkkel. Komoly kihívást és természetesen problémát jelent a TEMPEST követelményeknek való megfelelés is.

2. Nem minősített adatok védelme

Az eddigi áttekintés a minősített adat védelméről szólt, de létezik nem minősített, de védendő adat, illetve infrastruktúra, létesítmény.
2004 júniusában az Európai Tanács egy stratégia kidolgozását kérte a létfontosságú infrastruktúrák védelméről. Ennek eredményeképpen az Európai Közösségek Bizottsága 2004. október 20-án közleményt fogadott el „A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben" címmel.
Az Európai Unió Tanácsa 2005-ben határozatott hozott az információs rendszerek elleni támadásokról[38].
2005 november 17-én szintén a Bizottság zöld könyvet[39] fogadott el a létfontosságú infrastruktúrák védelmére vonatkozó európai programról, valamint döntött annak a figyelmeztető információs hálózatának[40] létrehozásáról.

2008.10.27-én az Európai Tanács határozatban szabályozta a létfontosságú infrastruktúrák figyelmeztető információs hálózatát[41].
2010. november 4-én sor került az első páneurópai kibergyakorlatra. Ezt a 2009-ben az Európai Bizottság közleménye tette lehetővé, ami a kritikus informatikai infrastruktúrák védelméről „Európa védelme a nagyszabású számítógépes

[38] A Tanács 2005/222/IB kerethatározata
[39] COM(2005) 576 végleges
[40] CIWIN - Critical Infrastructure Warning Information Network
[41] COM(2008) 676 végleges

támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”[42] címmel jelent meg.
2010. május 19. az Európai Unió a "Digitális Menetrend: A Bizottság akcióterve az európai jólét fellendítésére"[43] című közleményét jelentette meg.

A menetrend hét fontos területet emel ki:

- egységes digitális piac létrehozása
- az IKT [44] -termékek és -szolgáltatások közötti interoperabilitás keretfeltételeinek javítása
- az internet iránti bizalom és a biztonság erősítése
- jelentősen gyorsabb internet-hozzáférés biztosításának garantálása
- a kutatásra és a fejlesztés terén megvalósuló beruházások ösztönzése
- a digitális jártasság, a digitális készségek és a digitális inklúzió javítása
- az IKT-k alkalmazása az olyan társadalmi kihívások kezelése érdekében, mint az éghajlatváltozás, a növekvő egészségügyi költségek és az idősödő népesség.

A digitális menetrend célja volt, hogy létrehozzanak egy olyan rendszert, amely időben képes reagálni a számítógépes támadások ellen. Ennek keretében célként fogalmazták meg, hogy létrehozzák a CERT-ek hálózatát.
Az Európai Unión belül is léteztek szabályozások a kiber térben végbemenő cselekvésekre, de ezeket összhangba kellett és kell hozni a közösségen belül. Itt még problémásabb a helyzet, mert fizikai határok nem léteznek a kiber térben. Minden országban más és más törvények léteznek a szabályozásra. Természetesen van jogharmonizáció, de az eddigiekben nem volt arra példa, hogy a bűncselekmény elkövetésének helye, az elkövető, az elszenvedő és adott esetben az eszköz amivel elkövették egy azon időben máshol helyezkednek el. A szerverek lehet, hogy egy felhőben, egy virtuális térben léteznek, a hardverek több egymástól elkülönült helyen vannak elhelyezve. Természetesen ezen kívül van még egy fontos tényező, mégpedig az, hogy mindezek a helyszínek nem csak az EU-n belül lehetnek. Sok esetben ellenérdekelt országok vannak jelen a pókhálószerű rengetegben.
Szükséges megvédenünk a kritikus infrastruktúráinkat, amelyeket IT rendszerek tartanak működésben. Ezért nagyon fontos, hogy nemzetközi szerződésekben, olyan irányba tereljük a kibertérben történő cselekményeket, amelyek nem veszélyeztetik az előbb említett kritikus infrastruktúráinkat.

[42] COM(2009) 149
[43] IP-10-581_HU
[44] IKT: információs és kommunikációs technológia

Véleményem szerint minél inkább terheljük át az Internetes hálózatra mint átviteli közegre a kommunikációt, illetve minél inkább vesszünk igénybe egyre több szolgáltatást, amelyek az Interneten vannak, annál inkább nevezhetjük kritikus infrastruktúrának az Internetet magát. Komoly problémát jelentenek azok a kórházak, közintézmények amelyek az Internetet használják átviteli közegként, de okozhat fennakadást a különböző "tájékoztató honlapok" összeomlása is egy kritikus helyzetben. A digitális menetrend tartalmazza, hogy 2015-ig a lakosság 50%-a vegyen igénybe e-kormányzati szolgáltatásokat. Kérdéses, hogy mi van akkor, ha nincs Internet? Van az országnak üzlet folytonossági terve, katasztrófa terve? Hogyan lesznek összehangolva azok az intézmények, ahol megtalálhatók ugyan ezek a tervek, de nem számolnak az együttműködőekkel, akik a külső körülményekkel nem számolnak, vagy úgy gondolják, hogy az 100%-ban rendelkezésre áll minden időben.

A 2010-ben megfogalmazott Digitális Menetrendben meghatározott intézkedéseknek az első 3 évében kellett életbe lépniük. 2020-ra pedig az „Európa 2020" stratégia kiemelt kezdeményezéseként alakul és fejlődik tovább[45].

Az Európai Bizottság 2010 szeptemberében két új intézkedést jelentett be, amelyek elősegítené védekezést Európa kulcsfontosságú informatikai rendszereit fenyegető támadásokkal szemben. Az első intézkedés az Európai Parlament és Tanács Irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat hatályon kívül helyezéséről[46]. A kerethatározat hatályon kívül helyezése mellett célja volt a kiberbűnözés elleni küzdelem megerősítése azáltal, hogy közelebb hozta a tagállamok büntetőjogi rendszereit és szorgalmazta a hatóságok együttműködését. A második intézkedés Az Európai Parlament és a Tanács Rendelete az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA)[47]. Az ENISA hozzájárul, hogy az EU, az EU tagállamok és az üzleti szféra szereplői szakszerűbben tudják megelőzni és kezelni a kiberbiztonsággal kapcsolatos kihívásokat. [6]

Ugyancsak 2010-ben "Az Európai Bizottság Közleménye Az Európai Parlamentnek és a Tanácsnak az EU belső biztonsági stratégiájának megvalósítása: öt lépés a biztonságosabb Európa felé"[48] címmel kiadott dokumentumával szintén célként határozta meg az informatikai hálózatok biztonságának növelését.

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

[45] COM(2010) 245
[46] COM(2010) 517
[47] COM(2010) 521
[48] COM(2010) 673

- "Kapacitásépítés a bűnüldözés és az igazságszolgáltatás terén", amely keretében számítástechnikai bűnözéssel foglalkozó központot létrehozását jelentette be, amely többek közt kapcsolódási pontot jelent a nemzeti CERT-ek közt.
- "Együttműködés az iparral a polgárok eszközökkel való felruházása és védelme érdekében" Ebben a pontban kiemelt figyelmet kapott az információáramlás, az információkhoz való könnyebb hozzáférés. A Bizottság valós idejű központi adatbázist hoz létre a tagállamok és az ipar erőforrásainak és bevált módszereinek megosztására.
- elemekként kell működniük egy egységes rendszerben.

Hazai tekintetben fontos rendeletnek számít a témában a 27/2004. IHM rendelet, amely meghatározta a Kritikus Infrastruktúrafogalmát: „Kritikus infrastruktúra: mindazon létesítmények, szolgáltatások - beleértve az elektronikus hírközlési es informatikai rendszereket -, amelyek működésképtelenné válása vagy megsemmisülése egyenként es együttesen jelentősen befolyásolhatja a nemzet biztonságát, az állampolgárok élet- es vagyonbiztonságát, a nemzetgazdaság es a közszolgáltatok működését."
A Kormány 1249/2010. határozatában az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról intézkedett. Eszerint kijelölte a belügyminisztert az európai kritikus infrastruktúra védelem nemzeti koordinációjáért. Továbbá egy munkacsoport létrehozására tett felhatalmazást. A munkacsoport feladataként határozta meg, hogy dolgozza ki az európai és nemzeti kritikus infrastruktúrák azonosításához szükséges kritériumrendszert. Továbbá a lehetséges európai kritikus infrastruktúrák üzemeltetőinek vagy tulajdonosainak bevonásával tegyen javaslatot a kijelölésre és a kijelölés felülvizsgálatára. [7]
2012-ben "törvényi szintre emelkedett" a létfontosságú rendszerek és létesítmények azonosítása, kijelölése és védelmével kapcsolatos jogi háttér.[49] Az európai, nemzeti létfontosságú rendszerelem kijelölése, valamint a nemzeti és európai rendszerek kapcsolatát és közös szabályozását is tárgyalja a joganyag. A törvénynek megszületett a végrehajtási kormányrendelete.[50] A végrehajtási

[49] 2012. évi CLXVI. törvény
[50] 65/2013. (III. 8.) Korm. rendelet

rendeletben egzakt meghatározások vannak például arra vonatkozólag, hogy miket kell a létfontosságú rendszereknek tekinteni, milyen együttműködések szükségesek. 2013-ban elkészült Magyarország Nemzeti Kiberbiztonsági Stratégiája. A stratégia összhangban van az Európai Parlament által 2012. november 22-én elfogadott, "A kiberbiztonságról és védelemről szóló", 2012/2096(INI) számú határozat ajánlásaikhoz, továbbá a 2013. február 7-én "Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér" című közleménnyel. A stratégia elkészítésekor figyelembe vették a NATO 2010 novemberében elfogadott Stratégiai Koncepcióját, a 2011 júniusában elfogadott Kibervédelmi Politikáját, valamint a 2010. november 19-20-ai lisszaboni és a 2012. május 20-21-ei chicagói NATO-csúcs dokumentumaiban megfogalmazott Szövetségi kibervédelmi elveket és célokat. [8]

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról szól. "Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme."[51]

Az elkövetkező legfőbb feladatok, amiket a törvény meghatároz, hogy az elektronikus információs rendszereket biztonsági osztályba kell sorolni, valamint meg kell határozni a szervezetünk biztonsági szintjét.

Több új gondolkodásmód is megjelenik a törvényben. Ilyen például, hogy a szervezet vezetője felelős az informatikai biztonságért még abban az esetben is, ha annak végrehajtását egy külső cégre bízta. Kiemelt figyelmet kapott az Oktatás-képzés, kutatás-fejlesztés is. A minősített adat védelméről szóló 2009. évi CLV. törvénnyel összhangban ahol minősített adatot kezelnek, meg kell teremteni a minősített adat védelméhez szükséges, az adat minősítési szintjének megfelelő személyi, fizikai és adminisztratív, valamint ha a szerv a minősített adatot elektronikus információs rendszeren kezeli, az szóló 2009. évi CLV. törvényben és az elektronikus információbiztonságról szóló törvényben és végrehajtásukra kiadott jogszabályokban meghatározott elektronikus biztonsági feltételeket. [9]

A kiberbiztonság elérése érdekében több szervezet felállítására is felhatalmazást ad a törvény:

- Nemzeti Kiberbiztonsági Koordinációs Tanács (Miniszterelnökség vezet)

[51] 2013. évi L. törvény

A Tanács a Miniszterelnökséget vezető államtitkár vezetésével és a Miniszterelnökség által delegált kiberkoordinátor támogatásával létezik:

- Nemzeti Kiberbiztonsági Fórum (Magas szintű szakmai, illetve nem kormányzati szereplők vezetőszintje.)
- Kiberbiztonság ágazati munkacsoport (egyes ágazati szakértők javaslattételi joggal és véleményezési lehetőséggel segítik a Tanács munkáját)

- Nemzeti Elektronikus Információvédelmi Hatóság (Nemzeti Fejlesztési Minisztérium)
  Biztonsági osztálybasorolásáért és a törvény alkalmazásáért felelős szervezet, hatóságként működik a 2013. évi L. törvény szerint meghatározott elektronikus rendszerek tekintetében.
- Nemzeti Biztonsági Felügyelet (Közigazgatási és Igazságügyi Minisztérium)
  Szakhatósági feladatkörrel bír (felkérésre sérülékenységi vizsgálatokat végez) a 2013. évi L. törvény szerint meghatározott elektronikus rendszerek tekintetében, de hatóságként a 2009-ben a Mavtv. szerinti minősített adatokat kezelő elektronikai rendszerek tekintetében.
- CERT - Computer Emergency Response Team
  - GovCERT-Hungary - kormányzati eseménykezelő központ (Nemzetbiztonsági Szakszolgálat)
    Feladata a kiberbiztonsági koordinációs tevékenység, együttműködés az ágazati CERT-ekkel (CSIRT-ekkel),megelőző tevékenység, incidensek észlelése, kezelése, kapcsolattartás a Hatósággal.
  - CIP-CERT Critical Infrastructure Protection (BM Országos Katasztrófavédelmi Főigazgatóság)
  - MIL-CERT Katonai CERT
  - Nemzeti CERT munkacsoport
    Feladata kidolgozni a nemzeti kiberbiztonsági akcióterveket, az incidenskezelő protokollokat, gyakorlatok szervezni, együttműködés koordinálása a CERT-ek közt, valamint a nemzetközi együttműködés koordinálása.

A törvényhez bár késve, de sorra jelennek meg a végrehajtási rendeletek is. Ilyen a 233/2013. Az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló Korm. rendelet. Továbbá a 301/2013. a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló Korm. rendelet.

Összegzés

A folyamatosan változó IT rendszerek és az azokra épülő folyamatok biztonságos használata megköveteli a jogi szabályozás kialakítását is. Nem elég a gyors változásokat lekövetni, hanem fontos, hogy meglegyen a nemzetközi szabályzással is a jogharmonizáció. Ez komoly kihívást jelent a különböző kultúrák, érdekeket képviselő és értékrendekkel rendelkező nemzetek közt kialakítani. A különbözőségek mellett az IT hálózat és a gazdasági érdekek miatti globalizáció ugyanis mégis egy egységet képvisel.

Felhasznált irodalom

[1] 1998. évi LXXXV. törvény részletes indoklása[52]
[2] 1. számú melléklet a 2009. évi CLV. törvényhez 1.
[3] 1. számú melléklet a 2009. évi CLV. törvényhez 2.
[4] 1. számú melléklet a 2009. évi CLV. törvényhez 3.
[5] 1. számú melléklet a 2009. évi CLV. törvényhez 4.
[6]
[7] http://www.enisa.europa.eu/about-enisa/activities
[8] 1249/2010. (XI. 19.) Korm. rendelet
[9] 1139/2013. (III. 21.) Korm. határozat
[10] A minősített adat védelméről szóló 2009. évi CLV. törvény 10. § (4) bekezdése
[11] Dr. Rajnai Zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23., ZMNE, Budapest, 2013.

[52] Jogtár

Dorkó Zsolt[53]: Szervezetek struktúrája-II.

Absztrakt
A cikk bemutatja a PhD jelölt értekezésének egy részét.

Abstract
The article presents parts of thesis PhD candidate's.

Bevezetés

Az I. rész általános anyaga jelen publikációval folytatódik, amelyben alapvetően egy konkrét szervezet, a rendőrség struktúrájával foglalkozom.

1. A rendőrség szervezeti struktúrája

A rendőrség strukturális jellemzőinek vizsgálatát célszerűnek tartom abból a fenti alapvetésemből megközelíteni, mely szerint a szervezet működését alapvetően meghatározza a szervezeti felépítés jellege, a feladatrendszere, illetőleg a gazdálkodásának a keretei.
Feladatrendszere alapján a rendőrség védi Magyarország belső társadalmi rendjét, a lakosságot és az anyagi javakat. Az Alaptörvény[54] funkcionális feladatköri meghatározása szerint, alapvető feladata a bűncselekmények megakadályozása, felderítése, a közbiztonság, a közrend és az államhatár rendjének védelme. Ezen kívül a határforgalom ellenőrzése, a terrorizmus elleni küzdelem és rá vonatkozó törvényben[55] meghatározott bűnmegelőzési, bűnfelderítési célú ellenőrzés. A fenti feladatrendszerre, funkcionális elvek szerint elhatárolva, három rendőrségi szervezeti egységet hoztak létre[56]. A rendőrség, az általános rendőrségi feladatok ellátására létrehozott szervre, a belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szervre, valamint a terrorizmust elhárító szervre tagozódik. Tehát az elsődleges munkamegosztás szintjén, a törvény[57] alapján megtörténik a funkcionális elv szerint elhatárolás, amely viszonylag a homogén szakterületekre bontja a rendőrséget. A strukturális jellemzők mindegyik szervnél hasonlóan jelennek meg, de a vizsgálatomat csak az általános rendőrségi feladatok ellátására

[53] Heves Megyei Rendőr-főkapitányság osztályvezető.
[54] Magyarország Alaptörvénye 46. Cikk (1)
[55] 1994. évi XXXIV. törvény a Rendőrségről
[56] 1994. évi XXXIV. törvény a Rendőrségről 4. § (2)
[57] 1994. évi XXXIV. törvény a Rendőrségről

létrehozott szerv esetén végzem el, mivel az értekezésem szempontjából ez a releváns közeg.
A fejezet bevezetőjében megállapítottam, hogy a szervezeti struktúra kialakítását döntően befolyásolják a szervezet működési- vagy munkafolyamatai, tevékenységének főbb típusai, illetve az alkalmazott irányítási, vezetési elvek, módszerek.
A rendőrség munkafolyamatai három fő kategóriába sorolhatók,[58] [OKTF 100.o] ezek a szolgálati, a szervezet-fenntartási, valamint a gazdasági-ellátási folyamatok. A Szolgálati folyamat, a szervezet céljaként meghatározottak teljesítésére irányuló rendvédelmi feladatokból, és az azokhoz közvetlenül kapcsolódó egyéb részfolyamatokból áll. Másképpen fogalmazva azokat a rendőrségi feladatokat foglalják magukban, amelyeket a feladatrendszerét meghatározó normák előírnak, illetve elvárnak. A Szervezet-fenntartási folyamat, a szervezeten belüli viszonyok kialakítását, működtetését, a környezeti kapcsolatát szolgálja. A fő folyamat részfolyamatokból áll, amelyek a szervezési és humán szakterületek alrendszerét képezik. A gazdasági-ellátási, vagy logisztikai folyamat, a szervezet működéséhez szükséges pénzügyi feltételeket teremti meg, teljesíti az ellátási és fenntartási feladatokat, biztosítja a műszaki- technikai eszközöket és berendezéseket, valamint megszervezi és végrehajtja azok működtetését. Részfolyamatai a gazdasági szakterületeket alkotják. Funkciója alapján támogató alrendszerként is definiálhatjuk ezt a folyamatot, amely a rendőrségi menedzsment reformok esetén az első számú célpontjai a piaci megoldásoknak, az értekezésem fő vizsgálati célpontját jelenti.
A rendőrség strukturális jellemzőit döntően meghatározza a vezetés specifikus jellege. A vezetési funkciók gyakorlása során fokozottan érvényesülnek a tevékenységből adódó hatalmi viszonyok, az alá-fölérendeltség, az egyszemélyi parancsnoki rendszer. A tevékenység esetenként életveszély helyzetben történik, végrehajtása magas fokú szakszerűséget, tervszerűséget és több szerv koordinált tevékenységét igényli, amely speciális irányítási rendszert és vezetési rendet követel meg. A rendőrség irányítási rendszerén a különböző szintű vezetőszervek azon kapcsolat és viszonyrendszerét értjük, amely biztosítja a magasabb szinten hozott vezetői döntések által kimunkált feladatok alsóbb szinteken történő végrehajtását. Vezetési rendjén a vezető szervek belső kapcsolatát és viszonyát értjük, amelynek alapján előkészítik és meghozzák a vezetői döntéseket, valamint

[58] Tansegédlet a rendőri vezetők továbbképzéséhez (2012. IX. 03. – 2012. XII. 15.) BM Oktatási, Képzési és Tudományszervezési Főigazgatóság, Nagykovácsi 2012.

kidolgozzák és kiadják az alárendelt szakmai szervek számára szükséges feladatokat és biztosítják a szakmai feladatok végrehajtását.
Korában megállapítottam, hogy a szervezetek nagyságrendje és a végrehajtandó feladatok jellege alapvetően determinálják, hogy a rendőrség milyen szervezeti, irányítási modelleket alkalmaz.
Lineáris szervezeti modellt alkalmazzák a kis létszámú, homogén jellegű feladatokat végrehajtó szervezeteknél. Ilyen rendszerben történik járőrök, járőr párok, bevetési csoportok, különböző ideiglenes jelleggel létrehozott szolgálati elemek vezetése. Jellemzője, hogy a szervezet élén álló parancsnok a szolgálati utat használja fel a szakirányítási feladatok végrehajtására is. A szervezetszerű helyettesek segítik és tehermentesítik a parancsnokot a vezető-irányító munka végzésében, illetve bizonyos funkcionális feladatok ellátását végzik a parancsnok felhatalmazása alapján. Az irányítás sajátossága, hogy az alárendelt szervezeti egységek vezetői bevonásra kerülnek a magasabb szervezeti szint vezetési folyamatába, a vezetési funkciók gyakorlása során tett helyzetelemzésük, javaslatuk beépülhet a saját feladatrendszerükbe. A modell alkalmazásával a rendőrség esetében is érvényesülnek struktúra tárgyalásánál bemutatott jellemzők, érvényesül a közvetlen kapcsolattartás a szervezeti szintek között, a gyors és megbízható információáramlás, az irányítási információk pontosabb lejuttatása, és torzulásmentes visszacsatolása. A modell kevésbé képes a szakterületek eltérő szakmai sajátosságait figyelembe venni, nehézkessé válik az egymástól nagy távolságra elhelyezkedő szervezeti egységek vezetése.
Törzskari struktúrát a rendőrségen közepesen bonyolult, közeli térbeni elhelyezkedéssel rendelkező szervezeti egységek, bevetési osztályok, ideiglenes csapaterős egységek vezetésében alkalmazzák, ahol is a parancsnok döntései előkésztését, a végrehajtás megszervezését különböző szakterületekre szakosodott beosztottak előadók, törzstisztek hajtják végre, azonban nem kapnak felhatalmazást az általuk művelt szakterületek szakmai irányítására, hanem minden irányítási jogkör a parancsnok kezében összpontosul. Az elöljáró vezető munkáját közvetlenül segítve részt vesznek a döntések kimunkálásában, a végrehajtás megszervezésében és irányításában, a feladatok végrehajtásának ellenőrzésében. A szakirányítási feladatokon túlmenően feladatul kaphatják egyes alsóbb szintű szervezeti egységek munkájának folyamatos figyelemmel kísérését, felügyeletét. Az összetartozó munkafolyamatokat és funkciókat figyelemmel kísérő személyeket törzskarba szervezik. A szervezeti modell előnye természetesen a rendőrség esetén is érvényesül, így a nagyfokú szakmai hozzáértés, a szakirányítás minőségi végrehajtása. Hátrányának tekinthető, hogy a szervezet élén álló vezetőnek széleskörű szakmai ismeretekkel és nagyfokú önállósággal kell rendelkeznie a

szerteágazó munkafolyamatok helyes összehangolásához. A szakmai területeken dolgozó törzskari beosztottak általában nem rendelkeznek önálló döntési jogosítványokkal, ezért szakmai képességük terén kevésbé tudnak kibontakozni. A szervezeten belül éppen ezért könnyen kialakulhatnak szakmai ellentétek, viták, amelyek gátolhatják az egységes irányítást.

A korábbi törzskari struktúrát a rendőrség szervezetirányítási rendszerében a funkcionális irányítási modell váltotta fel, melyben a függelmi kapcsolatok linearitása miatt különösen fontossá válik a mellérendelt vezetők, és szervek közötti folyamatos koordináció. A funkcionális vezetési modell biztosítja az egységes irányítást igénylő szervezetben a különböző szakterületek viszonylagos önállóságát, amely a szakterületek közötti koordináció nélkül könnyen konfliktushelyzeteket okozhat. Ez a modell biztosítja a központi szerv, a megyei - fővárosi rendőr-főkapitányságok, a rendőrkapitányság, és kirendeltség szervezetirányítási rendszerét. A funkcionális-törzskari modellben megmarad a szervezeti szintek közötti közvetlen vezető-vezető kapcsolat, azonban a szakmai irányító szervek a szakmai területek irányításához közvetlen felhatalmazással rendelkeznek, mégpedig úgy, hogy az irányítást az alsóbb szintű szervezet, felelős vezetőjének tájékoztatása mellett közvetlenül az alsóbb szervezeti szint szakirányító szerveihez juttatják el információikat. A helyes szakmai döntések meghozatalához lehetőséget kapnak a közvetlen információszerzésre, amit gyakran adatszolgáltatással, helyszíni ellenőrzéssel, beszámoltatással oldanak meg. A modell előnye a nagyfokú szakszerűség biztosításában, a homogén szakmai folyamatok egységes irányításában, a közvetlen szakmai tapasztalatok összegyűjtésében és átadásában áll. A vezetők szakmai hozzáértését kevésbé, de felelősségét és áttekintő képességét jobban igényli. A vezetők tájékoztatásának kötelezettsége kissé bürokratizálja a szervezeti szintek közötti viszonyokat.

A rendőrség irányítási rendszere a szervezeti hierarchiának megfelelően három vezetési szintre tagozódik. A felsőszintű a központi szerv az Országos Rendőr-főkapitányság, középszintű a megyei, fővárosi rendőr-főkapitányságok, alsószintű a rendőrkapitányság, kirendeltség. A szinteknek megfelelően elhelyezkedő vezető szervek egyben a vezetési rendszer hierarchikus viszonyaira utalnak, vagyis a felsőszintű vezető szerv középszintű, a középszintű vezetőszervek pedig alsószintű vezető szervet irányít. Az irányítás rendje két úton valósul meg. A szolgálati-elöljárói rendszer a szolgálati úton elhelyezkedő egyszemélyi parancsnoki rendnek megfelelően elöljárói-beosztotti viszonyt hoz létre a szervezethez tartozó állomány között. A szolgálati úton helyezkednek el a szervezet élén álló vezetők helyettesei is. A szakmai elöljárói rendszer szakirányítási vonalat képez a pontosan körülhatárolt szakterületeket irányító vezető szervek és szakmai vezetők között.

Mindezek alapján a rendvédelmi szervek irányítási rendszerében lineáris és funkcionális modellek vannak jelen, amelyben a lineáris vonalat a szolgálati és szakmai irányítási rendszerek felső szinttől a végrehajtás szintjéig mutató vonalas elrendezése adja, funkcionális jellegét pedig a szakterületenkénti elhatárolódás képezi. [59]

2. Az informatika helye a szervezeti struktúrában

Amint azt a fentiekben bemutattam a szervezetek struktúrájának mindegyike alkalmazza valamilyen mértékben a lineáris formát. Bemutattam azt is, hogy ez a modell a rendőrség irányítási rendszerének több szintjén is fellehető. Ennek döntő oka, hogy a rendőrség irányítási rendszerét alapvetően a meglévő függelmi kapcsolatrendszer determinálja, mivel a szervezeti hierarchia meghatározó lépcsőinél az egyértelműen tisztázott, kizárólagos függelmi kapcsolatok érvényesítése nélkülözhetetlen. Ezért fokozottan érvényesülnek a lineáris szervezeti modell jellemzői. E modellben a szervezeti hierarchia csúcsán hozott döntések a vertikális csatornákon jutnak el a végrehajtás szintjére, illetve ugyanez a csatorna áll rendelkezésre a visszacsatolásra is. A szervezeti hierarchiában található szintek számával, vagyis a vertikális differenciáltság bővülésével, növekszik az áttételek száma, ezért gyakran konfliktusok, ellentmondások árán jutnak el az információk, utasítások, parancsok a végrehajtás szintjére. Tehát a lineáris szervezeti modell a vertikális tagoltság növekedésével egyre érzéketlenebb a problémákra, ezért is mondhatjuk azt, hogy ez szervezeti forma nem problémaorientált. Ahogy azt megállapítottam a rendőrség szervezetirányítási rendszerében a funkcionális irányítási modell valósul meg, de a linearitás jellemzői markánsan jelen vannak, ezért különösen fontos az, hogy a szervezetben a funkcionalitás alapján elkülönült szervezeti elemek, a vertikális tagoltság mely szintjén helyezkednek el. Hiszen a vertikális differenciáltság különböző szintjei pontosan meghatározzák a szervezeti egység, szervezeti hierarchiában elfoglalt helyét és szerepét. A szervezeti hierarchia legfelső szintjén a felső vezetés áll, alatta helyezkednek el a szervezet elsődleges munkamegosztása alapján elkülönülő funkcionális területei és azok vezetői. Ezek a funkcionális területek azonban nem minden esetben teljesen homogének, ami további mélységi, vertikális szintek

[59] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi Szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal, HU ISSN 2060-0437); Dr. habil. Négyesi Imre: DIE UNTERSTÜTZUNG DER SOLDATEN MIT ECHTZEITDATEN (A KATONÁK TÁMOGATÁSA VALÓS IDEJŰ ADATOKKAL) (Hadmérnök on-line, VII. évfolyam (2012) 4. szám, 162-166. oldal, ISSN 1788-1919).

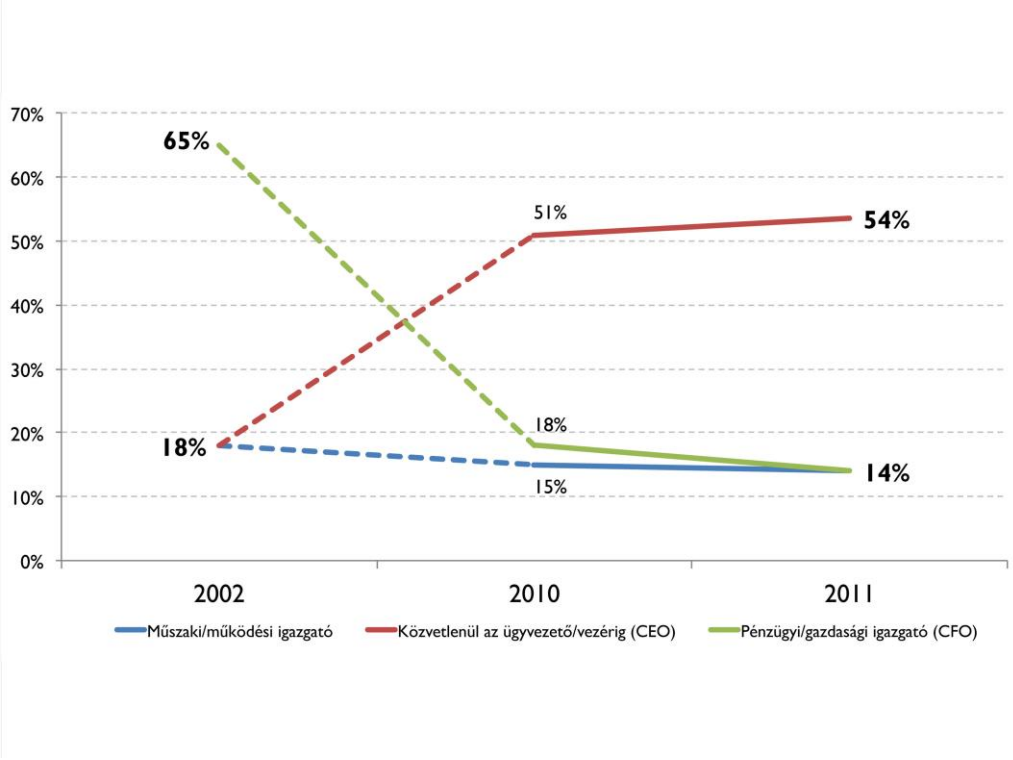
létrehozását teszi szükségessé. Ezek a szintek, illetve a vezetőik a hierarchiában elfoglalt pozíciójukból adódóan eltérő döntési jogosítványokkal rendelkeznek. A felsővezetői szint általában stratégiai kérdésekben dönt, irányokat, célokat határoz meg. A funkcionális vezetői szinten, a munkamegosztás alapján a szervezeti részterület, vagy egy teljes munkafolyamat tervezése, szervezése, koordinálása a vezető hatásköre. A mélységi tagoltság alsóbb szintjein is megmarad a funkcionálisan elkülönülő részterület felügyelete, de a szolgálati-elöljárói rendszerben az egyszemélyi parancsnoki rendnek megfelelően elöljárói-beosztotti viszony jön létre a felette álló funkcionális szerv vezetőjével. Ebből adódóan az egyes szintek vezetői az eltérő feladataikhoz eltérő hatáskörökkel rendelkeznek. Ez az oka annak, hogy szervezeti struktúra különböző szintjei pontosan meghatározzák, hogy a szervezeti egység, szervezeti hierarchiában elfoglalt helyét és szerepét. Tehát, ha megvizsgáljuk egy szervezeti egység szervezeten belüli elhelyezkedését, pontos képet kaphatunk arról, hogy az milyen szerepet tölt a szervezetben.

Az informatika rendőrségen belül elfoglalt helyét vizsgálva azt tapasztaltam, hogy pozíciója az idők során jelentősen megváltozott. Gondolatmenetem zárását előrevetítve, ez a pozíció véleményem szerint általában nem volt összhangban a szakterület szervezetre gyakorolt és a szervezetet jelentősen determináló pozíciójával. A kutatásom időintervallumában az informatika, illetve az elődszervezetei döntően három jól körülhatárolható pozícióban voltak, amely pozíciók a szakterület, illetve a vezetői hierarchiában elfoglalt helyét is meghatározták. A vizsgált időszakban a szakterület közvetlenül a szervezet vezetőjének, a műszaki szakterület vezetőjének, illetve a gazdasági terület vezetőjének alárendelt funkcionális szakterületként működött. A szakterület szervezetben elfoglalt pozícióját a rendőrség szervezeti felépítését részletesen taglaló fejezetben mutattam be.

Szükségesnek tartom megvizsgálni azt is, hogy az államháztartáson kívüli szervezetek, vállalatok esetében, hol foglal helyet az informatika. A témához kapcsolódóan a kis- és középvállalatok valamint a nagyvállalatok körében a Budapesti Corvinus Egyetem és az ITSMF[60] készített több, közös kérdőíves kutatást. A kutatások az informatikai szakterület szervezetben elfoglalt helyét, a szervezet informatikai felsővezetőjének pozícióját középpontba állítva vizsgálják, melynek eredményeképpen azt a kérdést teszik fel, hogy „Kinek jelent, az informatikai vezető? ” A felmérések eredményeiként három kategóriába lehet sorolni azt, hogy

[60] IT Service Management Forum

kinek jelent az informatikai vezető. Ezek alapján jelenthet közvetlenül a vezérigazgatónak, a gazdasági/pénzügyi igazgatónak, illetve a műszaki/működési igazgatónak.



1.számú ábra
forrás: [http://tudman.files.wordpress.com/2011/11/kutatc3a1sijelentc3a9s2011.pdf]

Fehér Péter[61] a kutatás egyik résztvevője szerint mindegyik pozíciónak van logikus magyarázata. A vezérigazgatónak való közvetlen kapcsolódás azt jelenti, hogy az informatikának a szervezeten belül jelentős súlya és stratégiai szerepe van, valamint egyenrangú a szervezet többi területével. A stratégiai szerepkörbe került informatika meghatározó tényezője a szervezet sikerességének. A műszaki/működési igazgatónak való alárendelésnek világos a logikája, hiszen az informatika egyrészt technológia, másrészt az alapvető működés része. E

[61]Dr. Fehér Péter közgazdász, kutató, tanácsadó, a Budapesti Corvinus Egyetem docense.

gondolatmenet eredményeképpen a termékek, illetve a szolgáltatások előállításáért, az ennek érdekében végzett tevékenység hatékony, gazdaságos végrehajtásáért elsősorban a műszaki/működési igazgató a felelős. E tevékenységi kör nem nélkülözheti az informatikai szakterület, mert az elválaszthatatlan része az alapfolyamatoknak. Az informatikának e területre való pozícionálása egy erős termelői, termelési informatikai szemléletet takar, ahol az informatika, mint termelési/produktivitási eszköz jelenik meg. Pénzügyi igazgató alá tartozás logikusnak tűnő magyarázata az lehet, hogy az informatika szakterület működtetése látszólag és viszonylagosa sokba kerül, így az jelentős költségtényező. Az, hogy a szakterület a gazdasági/pénzügyi igazgató alá tartozik egyet jelent azzal, hogy az informatika nem más, mint egy egyszerű költséghely, és nem stratégiai eszköz. Az informatika felügyeletét általában ott látja el a gazdasági/pénzügyi vezető ahol az informatika elsősorban költséghely, költségtényező, és alapvetően „csak" az üzemeltetési feladatokhoz kapcsolódik.

A grafikont tanulmányozva az alábbi következtetések vonhatók le:

A 2000-es évektől megfigyelhető, hogy a szervezetek informatikai felsővezetői feljebb kerülnek a szervezeti hierarchiában. A felmérés igazolta, hogy egyre inkább a vezérigazgató közvetlen irányítása alatt működik az informatikai szakterület, tehát a vezetője közvetlenül a vezérigazgatónak tartozik beszámolási kötelezettséggel. 10 év alatt 18 %-ról, 54 %-ra növekedett a szervezet vezetőjének jelentő informatikai vezetők száma. A szervezetben elfoglalt és magas státusza azt eredményezi, hogy folyamatosan növekszik az informatika elfogadottsága. A stratégiai szerepkörbe került informatika meghatározó tényezője lehet a szervezet sikerének. Ez a szervezeti megoldás jelzi az informatika szervezeti fontosságát, egyenrangúságát a többi funkcionális területtel.

A gazdasági/pénzügyi igazgató alá tartozás erős csökkenő tendenciát mutat, szinte inverze a szervezet vezetője alá tartozás tendenciájának. 10 év alatt 65 %-ról 14 %-ra csökkent azoknak a szervezeteknek az aránya melyeket a gazdasági vezetőnek jelentenek. Az, hogy a gazdasági vezetőnek jelentő informatikai felsővezetők a továbbiakban a szervezet vezetőjének közvetlen alárendeltségébe kerültek azt eredményezte, hogy a szervezeti hierarchiában elfoglalt helyük megegyezik azzal a szinttel, amelynek korábban alárendelt szervezeti egységei voltak, tehát a gazdasági vezetővel kerültek egy szintre. A kutatás eredményei azt mutatják, az szakterület képesek volt megszabadulni attól a szemlélettől, hogy az informatika nem más, mint egy költséghely a szervezet költségvetésében. A válság alatt 2008-ban látható volt egy csekély mértékű visszarendeződés, az informatika ismét több helyen visszakerült az költségkategóriába, azonban a trend nem fordult meg.

A műszaki igazgatóhoz való tartozás mértéke állandósulni látszik a 14 %-os szinten. Az elmúl 10 évben ez 4 % pontos csökkenést mutat. feladatokon túlmutató üzemeltetési pozícióhoz tartozás a válságtól függetlenül növekvő tendenciát mutat. A műszaki/üzemeltetési igazgató alárendeltségében működő informatikai szervezetnél a műszaki tartalomról az üzemeltetésre kerül át a hangsúly, ezekben az esetekbe az informatika jellemzően közmű jellegű. Inkább csak elméleti jellegű az a megközelítés mely szerint amennyiben az informatika a műszaki/üzemeltetési vezető alá tartozik úgy nehezebben jut forrásokhoz, mintha a vezérigazgató, vagy a gazdasági igazgató közvetlen irányítása alatt látná el a feladatát. Másik megközelítés szerin pénzügyi vezető sokkal keményebben bánik a hozzá tartozó területekkel. Tehát ebből a szempontból nem jelent egyértelmű hátrányt a műszaki szakterület alá tartozás. A grafikon adatai az utóbbi években nem tartalmazzák 100 %-ban az informatikai szervezetek hovatartozását. Ennek az oka az, hogy a kutatásokban is vizsgált 3 fő kategória mellett azonosítható még 2 speciális helyzetet. Az egyik, amikor az informatika az anyavállalati informatikai vezetőnek jelent. Ez általában, a multinacionális nagyvállalatok esetében tapasztalhatót, amikor az informatika lokálisan működik, de a nagyfokú centralizáltság miatt az informatikai prioritások, irányok mégis külföldön kerülnek meghatározásra. A másik speciális eset, amikor az informatika a szolgáltató központ vezetőnek jelent. Ezek a szolgáltató központok nem feltétlenül csak informatikai szolgáltatásokat nyújtva, a vállalatok mellett alakulnak, vagy telepszenek meg. A szolgáltató központ vezetője a szervezet vezetőjének jogait csak korlátozottan gyakorolhatja, ezért a felmérés külön kezeli ezt az esetet.

Az informatika szervezeti struktúrában elfoglalt szerepének vizsgálatát összefoglalva, bizonyítottnak vélem azt a korábbi megállapításomat, mely szerint a gazdaság szinte minden területe az informatika által vezérelt „iparággá" vált. Oly mértékben van jelen az informatika a legtöbb szervezetben, hogy bármilyen változtatás a szervezet alaptevékenységében azonnal változást indukál az informatikai rendszerben is. Általánosságban elmondható, hogy ha nem informatikai eszközök bevonásával valósítják meg változtatást, akkor romlik a szervezet hatékonysága. Tehát az informatika lényegében a szervezetek pótolhatatlan elemévé vált. Látható az, hogy az informatikai szakterület, illetve a területet menedzselő informatikusok, majd a későbbiekben informatikai vezetők, hosszú evolúciós utat jártak be. Kezdetben, mint üzemeltetési vezetők, mintegy csatolt munkakörként felügyelték az informatikát. Ebben az időszakban az elektromos hálózat üzemeltetése mellet, mellékesen ellátták a számítógépek üzemben tartását. Majd, mint önálló szakterületet felügyelő vezetők, a műszaki-üzemeltetési, vagy a gazdasági-pénzügyi terület beosztott szakterületeként

üzemeltették a szervezetük informatikai infrastruktúráját. Sajnos ez az utóbbi nézet elég mélyen begyökerezett néhány szervezet struktúrájába, hiszen sok szervezetnél még ma is úgy tekintenek az informatikára, mint egy támogató szervezetre, melynek elsődleges feladata a rendelkezésre álló informatikai infrastruktúra zavartalan üzemeltetetésének biztosítása. Természetesen ez az üzemeltetői háttértámogató szerep sem nélkülözhető, de a szervezetek érdeke nem ezt diktálja. Az elmúlt évtizedben az informatika a legtöbb szervezetben túlnőtt háttértámogatói szerepén, elválaszthatatlan része lett az alapfolyamatoknak, közvetlenül támogatva a szervezet feladatrendszerét. A feladatrendszerének átalakulásával az informatika a legtöbb szervezetben megkerülhetetlen stratégiai szerepkörbe került. Ez a szerepkör azt jelenti, hogy kikérik a véleményét minden szervezeti, strukturális változtatás megtervezéséhez és kivitelezéséhez, mivel minden változtatás mögött ott rejlik az azt támogató informatikai rendszer, amelyre a módosításokat le kell képezni. Ott ahol a döntéshozók felismerik az informatika stratégiai szerepét és bevonják a tervezési fázisba is, változtatások zökkenőmentes végrehajthatóak. Ez azonban nemcsak lehetőséget teremt az informatikai szervezetnek, hanem felelősséget is jelent, melynek csak akkor tud megfelelni, ha munkamegosztás alapján megfelelő hatáskörrel is rendelkezik. A kicsit túlzóan evolúciónak nevezett folyamat eredménye az, hogy az informatika közvetlenül a szervezet vezetőjének az irányítása alatt látja el a feladatát, tehát a vezetője neki jelent, ami azt eredményezi a szervezeti hierarchiában elfoglalt helyük megteremti, vagy megteremtheti azt a hatáskört mellyel meg tud felelni a stratégiai szerepkörének. A fenti kutatás egyértelműen alátámasztja azt, hogy a döntéshozók felismerték az informatika fontosságát, hiszen a század eleje óta tart az a trend, mellyel az informatikai kiléphetett az egyszerű költséghely besorolásból. A trend jellemzője, hogy az informatikai vezetők egyre inkább közvetlenül a szervezet vezetőjéhez tartoznak, miközben a pénzügyi szemléletet tükröző gazdasági vezető alá való tartozás mértéke folyamatosan csökken. Napjainkban az informatika stratégiai jelentőségét jól mutatja, hogy az informatikai vezetők 54 %-a közvetlenül a szervezet vezetőjéhez tartozik. Ez a szervezeti megoldás egyértelműen jelzi az informatika szervezeti fontosságát, és egyenrangúságát a többi funkcionális területtel.

Összegzés

Jelen cikk bemutatta a szerző PhD értekezésének egy második részét, amely a szervezetek alapvető struktúráit követően a rendőrség lehetőségeit mutatta be.

Felhasznált irodalom

A lábjegyzetekben.

Jelen számunk szerzői

Dorkó Zsolt	NKE PhD hallgató
Hullán Szabolcs	OE PhD hallgató
Mógor Tamásné	OE PhD hallgató
Puskás Béla	OE PhD hallgató
Dr. Rajnai Zoltán	OE egyetemi tanár
Szabó Anna Barbara	OE PhD hallgató
Szente András	OE PhD hallgató
Solymosi János	OE PhD hallgató
Zele Balázs	OE PhD hallgató

Szerzőink figyelmébe

Kiadványunk lehetőséget biztosít max. 40 ezer leütés (egy szerzői ív) terjedelemben – *elsősorban: távközlés, híradás, informatika, információvédelem, illetőleg hadtudományi és természettudományi témakörökben* – tanulmányok, szakcikkek magyar és idegen nyelvű megjelentetésére.

A cikknek tartalmaznia kell egy 2-5 soros absztraktot magyar és idegen nyelven.

A cikkek beküldése e-mailen a hhk_hirado_szakcsoport@uni-nke.hu címre lehetséges. A cikkek leadási határideje: folyamatos (megjelenés évente kétszer).

A megjelentetésre szánt cikkek csak a szerző(k) eddig máshol még meg nem jelent, saját önálló (társszerzők esetében közös) írásműve(i) lehetnek. Az írásművekben lévő idézeteknek meg kell felelniük a szerzői jogról szóló hatályos jogszabályoknak. A megjelentetésre szánt írásművek csak nyílt (nem minősített) információkat és adatokat tartalmazhatnak. Ezek minősített voltát a szerkesztőbizottság nem vizsgálja, ennek felelőssége a cikk szerzőjét terheli.

A szerkesztőbizottság a megjelentetésre szánt írásműveket lektoráltatja. A szerkesztőbizottság fenntartja a jogot, hogy a megjelentetésre szánt és megküldött írásművet – *külön indoklás nélkül* - megjelenésre alkalmatlannak ítélje. Az ilyen cikkeket nem küldi vissza, és nem őrzi meg.

A kiadványban lehetőség van idegen nyelvű cikkek megjelentetésére. Az idegen nyelven megjelentetésre szánt írásművek nyelvi lektorálása a szerzőt terheli.

Minden kézirathoz elektronikusan is mellékelni kell egy kitöltött "Kéziratbeküldési űrlap"-ot, és egy "Copyright átruházási űrlap"-ot. Mindkét űrlapot ki kell nyomtatni és alá kell írni (többszerzős cikk esetében minden szerzőnek!), majd a kinyomtatott és aláírt űrlapokat faxon (fax szám: +36-1-432-9025), vagy postai úton levélben (levélcím: Hírvillám Szerkesztőség, 1581. Budapest Pf.: 15.) is meg kell küldeni a szerkesztőségnek. Ezek hiányában a cikkeket a szerkesztőség nem lektoráltatja és nem jelenteti meg!

Az űrlapok a szerkesztőségnél szerezhetők be.

Felelős kiadó: Dr. Fekete Károly mk. alezredes
Megjelent az NKE HHK Híradó Tanszék gondozásában, 10 példányban, illetve elektronikusan:

www.puskashirbaje.hu

HU ISSN 2061-9499

***

NKE HHK Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf. 15.
+36 1 432 9000 (29-358 mellék)
hhk_hirado_szakcsoport@uni-nke.hu