Műszaki Katonai Közlöny

XXVI. évfolyam, 2016. 2. szám

Megyeri Lajos[1]

ADATOK BIZALMASSÁGÁNAK, SÉRTETLENSÉGÉNEK ÉS RENDELKEZÉSRE ÁLLÁSÁNAK BIZTOSÍTÁSA KATONAI INFORMÁCIÓS RENDSZEREK ALKALMAZÁSA ESETÉN

(DATA CONFDENTALITY, INTEGRITY AND AVAILABILITY OF INSURANCE IN CASE OF THE USE OF MILITARYINFORMATION SYSTEMS)

Az információk védelmének igénye egyidős a kommunikáció megjelenésével. Különösen igaz ez a megállapítás az állam számára fontos katonai információk kezelésekor. A XXI század technikai eszközeinek a nagymértékű „informatizálódása" óriási mértékben meggyorsította az információáramlást. Új adattovábbítási eljárásokat valósítottak meg, melyek gyökeresen megváltoztatták a katonai hírközlési rendszerek felépítését és jelentősen megnövelték az általuk nyújtott szolgáltatásokat. Jelen cikkében a szerző elemezni kívánja a különböző információs rendszerek működését az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának szempontjából, a rendszerek működtetésére fordított emberi és anyagi erőforrások figyelembevételével.

Kulcsszavak: *Információ, bizalmasság, elérhetőség, sértetlenség, minősített információ, továbbítás, védelem, rendszabályok*

The need to protect information is as old as the advent of communication. This is especially true for the country when it handle important military information. Technical equipment of XXI century, the high level of IT use vastly accelerated the flow of information. New data transmission procedures were implemented, which radically changed the structure of the military communications systems have significantly improved their services. The author in this article analyze the operation of the different information systems, data confidentiality, integrity and availability of point of view, taking into account the operation of the systems at the human and material resources.

Keywords: *Information, confidentiality, availability, integrity, classified information, transmission, security, protection, rules*

BEVEZETŐ

Az információ biztonság kérdése már a rádiók használatának elterjedésével egy időben megfogalmazódott. Baros Ödön százados a Rádió a közbiztonság szolgálatában című jegyzetében 1943-ban megfogalmazta a rádiótávírász csendőrök által követendő szabályokat [1]. Ebben az időben kezdődött a géptávíró pályafutása is. Alkalmazásával lehetőség nyílt az ínformáció leírt formában történő továbbítására.

A szembenálló felek természetesen az első híradó eszköz megjelenésével egy időben rájöttek arra, hogy a másik fél kommunikációja megzavarható, félrevezethető, lehallgatható. Mind-

[1] Nemzeti Közszolgálati Egyetem, doktorandusz. E-mail: megyeri.lajos@uni-nke.hu ORCID: 0000-0002-3743-1520

ezek megakadályozására különböző technikai megoldásokat alkalmaztak és a közlemények továbbítására szabályokat dolgoztak ki.

A mikroelektronika fejlődésével, a mikroprocesszorok széles körű alkalmazásával megváltozott a számítógép és vele együtt az informatika fogalma. A fejlett logikai áramköröket beépítették híradó, műszaki, fegyverirányítási, gépjármű és még számtalan más terület eszközeibe. Minden terület „informatizálódott" bizonyos mértékben.

Az információs rendszerek védelmének szükségessége magától értetődő, különösen katonai alkalmazások esetén. Fontosnak tartom megvizsgálni e tekintetben a hazai és NATO szabályozás rendszerét, hogy a későbbiekben összehasonlíthassam a polgári információs rendszerek működésének szabályozásával, lehetőségeket keresve a katonai és nem katonai információs rendszerek összekapcsolási lehetőségeire, a hatékonyság növelése és üzemeltetési költségek optimalizálása érdekében, a biztonsági szempontok teljes figyelembevételével.

Ennek keretében jelen cikkben tanulmányoztam és összehasonlítottam a nemzeti és NATO Információbiztonsági szabályozókat annak megállapítására, hogy a cikk címében megfogalmazott alapelvek hogyan érvényesülnek az információs rendszerek teljes életciklusában.

A katonai infókommunikációval részletesen foglalkozik Munk Sándor [2]. Az információbiztonság kérdéseivel foglalkozik Kassai Károly [3], Haig Zsolt [4] és Muha Lajos [5]. Mindannyian a téma hazai ismerői.

1. NYÍLT (NEM MINŐSÍTETT) INFORMÁCIÓS RENDSZEREK

Először határoljuk be a vizsgálandó területet, határozzuk meg az információs rendszer fogalmát. A NATO szakterületi (híradó és informatikai) fogalomjegyzéke szerint:

„*Az információs rendszer eszközök, módszerek, eljárások, illetve szükség esetén a működtető személyzet információ feldolgozási funkciók megvalósítására létrehozott rendszere*" [6]. Ez meglehetősen tág meghatározás. Jelen cikkben, a terület pontos behatárolása érdekében az információs rendszer fogalma alatt informatikai eszközökkel létesített kommunikációs rendszert értek majd. Bár a szoftverrádiók korában az informatikai eszközök egyértelmű szétválasztása is nehéz, a rádióhullámok segítségével hang alapú kommunikációt szolgáltató rendszerekkel más alkalommal kívánok részletesen foglalkozni.

A nyílt információ definíciója igen egyszerű. Minden információ nyílt, amely nincs minősítve [7]. A minősített információ fogalomkörét a második fejezetben részletezem. A következőkben értelmezem a bizalmasság, sértetlenség és rendelkezésre állás fogalomkörét.

Bizalmasság: Azt jelenti, hogy az információs rendszerben tárolt adathoz csak az arra jogosult személyek kezelhetik a jogosultságuknak megfelelő mértékben. Nyílt adatkezelő rendszerekben gyakori a központi adattárolás, ahol egy adott adatbázishoz, (például az alakulathoz érkezett ügyiratok könyvtára) a rendszer valamennyi felhasználója hozzáférhet. Ez gyors adatcserét, hatékony munkavégzést tesz lehetővé. Hátrány lehet, hogy egyes felhasználók nem csak a saját munkájukhoz szükséges információkat ismerik meg. Mivel az adatok nem minősítettek, ez nem jelent titoksértést. Az adatbázist frissítő állománynak nagy figyelmet kell fordítania arra, hogy személyiségi jogokat sértő (például egészségügyi, bűnügyi) adatok erre a nyílt

rendszerre ne kerülhessenek fel. Jó megoldást jelent a Honvédségnél rendszeresített információ menedzsment rendszer (IMR) szoftver, amely bár nyílt adatokat kezel, a programban meghatározható, hogy egyes adatokhoz mely személyek férjenek hozzá.A hozzáférés tényét, a tett intézkedéseket, az ügy kapcsán készült ügyiratokat az IMR rendszer visszakereshető formában dokumentálja.

Sértetlenség: Azt jelenti, hogy a rendszerben kezelt adat a jogosult felhasználó által készítettel megegyezik minden tulajdonságában. Ennek biztosítása nyílt adatkezelő rendszerekben a felhasználók jelszó/felhasználó név azonosításával történik. Minden felhasználó figyelmét fel kell hívni arra, hogy felhasználói adatait senkinek ne adja át, mert így biztosítható az adatkezelési eljárások pontos névhez kötése.

Rendelkezésre állás: Azt jelenti, hogy a felhasználó az informatikai rendszerben tárolt adataihoz a munkája ellátásához szükséges mértékben bármikor hozzáférhessen. Nyílt informatikai rendszerekben ez viszonylag könnyen kivitelezhető, meghibásodott rendszerelemek hardver, szoftver frissítése, javítása, pótlása viszonylag egyszerűen, alapvető logisztikai szabályok betartásával megoldható.

Az információs rendszerek tervezésére, kivitelezésére, üzemeltetésére, használatára, karbantartására és felszámolására az alábbi szabályok az irányadók:

Nem minősített adatok elektronikus úton történő továbbítása esetén a polgári szabályozás alapját az MSZ/ISO 27000 szabvány képezi. Ezt a szabványcsaládot a Brit 7799 szabványcsalád alapján készítették.

Az információbiztonsági irányítási rendszer (továbbiakban IBIR) feladata az információk bizalmasságának, sértetlenségének és rendelkezésre állásásának megőrzése. A rendszer része a kockázatkezelési folyamat is.

Az IBIR alkalmazása lehetővé teszi, hogy a különböző informatikai hálózatok tervezői, kivitelezői és üzemeltetői egységes keretrendszerben gondolkodjanak, a szakmai folyamatokat és kifejezéseket azonos módon értelmezzék. A szabvány alkalmazásával tervezett és működtetett rendszerek megfelelőségi tanúsítványt szerezhetnek, ezzel növelhetik a bizalmat a rendszer megbízhatóságával, bizalmasságával és rendelkezésre állásával kapcsolatban.

A katonai információtovábbítás lényegében követi az MSZ/ISO 27000 szabványban foglaltakat [8], csak ahogy a hadseregekben szokás, egyértelmű parancsokat és utasításokat adtak ki az egységes értelmezés érdekében.

A 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról értelmezi az információbiztonság területén használatos fogalmakat, az egyes feladatkörökhöz tartozó beosztások megnevezését, függelmi viszonyait [9]. Meghatározza az információbiztonsági célokat és alapelveket, egyértelműen értelmezi az adatkezelő rendszerek üzemeltetéséhez szükséges személyek felelősségi körét és feladatait. Új elemként jelenik meg az utasításban, hogy a honvédelmi szervezeteknél az adatokat a bizalmasságuk szerint biztonsági osztályokba kell sorolni a következők szerint:

„*a) alap biztonsági osztályba kell sorolni a nem minősített adatot;*

b) fokozott biztonsági osztályba kell sorolni a nem minősített nagy mennyiségű személyes adatot, a különleges adatot, az üzleti adatot, a címtáradatot az üzemeltetési adatot a magasabb szintű biztonsági követelmények alkalmazása érdekében;

c) korlátozott terjesztésű biztonsági osztályba kell sorolni a jogszabály szerint "Korlátozott terjesztésű" minősítésű adatot;

d) bizalmas biztonsági osztályba kell sorolni a jogszabály szerint "Bizalmas" minősítésű adatot;

e) titkos adat biztonsági osztályba kell sorolni jogszabály szerint "Titkos" minősítésű adatot;

f) szigorúan titkos adat biztonsági osztályba kell sorolni jogszabály szerint "szigorúan titkos" minősítésű adatot."[10]

Az utasítás értelmében az adatkezelő rendszer által kezelt adatoknak, iratoknak az adat-, iratkezelés minden fázisában - papíralapú és gépi adathordozó esetében egyaránt - biztosítani kell a biztonsági osztályba sorolásra vonatkozó védelmet.

A 3/2012. (I. 13.) HM utasítás [11] pontosította a védelmi intézkedéseket, és előírta, hogy „*a biztonsági követelményeket meghatározott védelmi rendszabályokon és kialakított eljárásokon keresztül kell érvényesíteni, amelyeket Elektronikus Információbiztonsági Szabályzat (a továbbiakban: EIBSZ) formájában kell megfogalmazni, jóváhagyatni és alkalmazni*"

Mindezek alapján a nem minősített adatokat feldolgozó informatikai rendszerekkel szemben is elvárásokat támaszt, követelményeket határoz meg, ennek alapján működik például a Magyar Honvédség zárt informatikai rendszere is. Az EIBSZ az adatok megfelelő bizalmasságának, sértetlenségének és rendelkezésre állását biztosító helyi szabályozást részletesen tartalmazza. A szabályzatot a rendszer valamennyi felhasználójának ismernie kell, és évente legalább egy alkalommal foglalkozás keretében frissíteni az ismereteket.

Minden egyes informatikai rendszernek rendelkeznie kell minden helyszínen egy helyi EIBSZ szabályzattal.

2. MINŐSÍTETT INFORMÁCIÓS RENDSZEREK

A 2009. évi CLV. számú, a minősített adat védelméről szóló törvény 3.§ [12] szerint minősített adatok a következők:

„*a) nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - a megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza;*

b) külföldi minősített adat: az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza"

Bizalmasság: Azt jelenti, hogy az információs rendszerben tárolt adathoz csak az arra jogosult személyek kezelhetik a jogosultságuknak megfelelő mértékben. Minősített adatkezelő rendszerekben gyakori a „system high" üzemmód alkalmazása, ami azt jelenti, hogy a rendszerben kezelt valamennyi adatnak megvan a legmagasabb alkalmazható minősítési szintje, és a rendszer valamennyi felhasználójának rendelkeznie kell erre a minősítési szintre érvényes felhasználói engedéllyel. Ettől függetlenül mindenki felhasználó név/ jelszó alkalmazásával lép be a rendszerbe és nem láthatják egymás mappáit, csak a megosztottakat.

Sértetlenség: Azt jelenti, hogy a rendszerben kezelt adat a jogosult felhasználó által készítettel megegyezik minden tulajdonságában. Ennek biztosítása a minősített adatkezelő rendszerekben is a felhasználók jelszó/felhasználó név azonosításával történik. Minden felhasználó figyelmét fel kell hívni arra, hogy felhasználói adatait senkinek ne adja át, mert Ha megteszi, minősített adattal való visszaélés következhet be, amelynek súlyos jogi következményei vannak.

Rendelkezésre állás: Azt jelenti, hogy a felhasználó az informatikai rendszerben tárolt adataihoz a munkája ellátásához szükséges mértékben bármikor hozzáférhessen. Minősített informatikai rendszerekben ez nagy nehézségekbe ütközhet. Meghibásodás esetén a hardverszoftver konfiguráció cseréje, változtatása engedély köteles. Bizonyos különleges részegységek (TEMPEST [13] tanúsítvánnyal rendelkező konfigurációk) nem cserélhetők részeiben, csak teljes készletben. Ezért a rendelkezésre állás biztosításának megszervezése nagy körültekintést és anyagi kapacitást igényel.

A 2009. évi CLV. számú, a minősített adat védelméről szóló törvény részletesen leírja a minősítők körét, a minősítési eljárást, az alkalmazott jelöléseket és a minősített adat biztonságára vonatkozó általános szabályokat.

A törvény nagy jelentőségű újdonsága, hogy a nemzeti minősített adatok kezelésére ugyanolyan rendszabályok alkalmazását írja elő, mint a külföldi minősített adatok esetében. A törvény hatályba lépéséig a nemzeti minősített adatok védelmére nem voltak olyan szigorú fizikai biztonsági követelmények előírva, mint például a NATO adatok védelme esetében.

Hazánk NATO csatlakozása után a NATO információbiztonsági követelményeket a C-M(2002)49 direktíva [14] fogalmazta meg. Ennek alapján kezdődött a NATO minősített információk tárolására, feldolgozásra akkreditált „NATO T irodák" kialakítása nagy anyagi ráfordítással. Kényszerpályán voltunk, mondhatnánk szerencsére, mert a NATO csak akkor volt hajlandó minősített információ átadására az új tagország – Magyarország – felé, ha megteremtjük a személyi, fizikai és adminisztratív feltételeket, melyeket valamennyi tagállamtól elvár a szövetség. Az állam kénytelen volt megteremteni a feltételeket, amelyek azonban csak

a NATO minősített adatokra vonatkoztak. Saját nemzeti minősített adatainkat a régebbi előírások szerinti, jóval szerényebb védelmet biztosító feltételek szerint kezelhettük.

A 2009. évi CLV. számú törvény megszüntette ezt a kettősséget és a nemzeti adatok védelmére is a külföldi (lásd NATO) védelmi rendszabályokat léptette életbe. Ez a módosítás rövidtávon sok gondot okozott a döntéshozó és végrehajtó állománynak egyaránt. A nagy fizikai védelmet nyújtó védelmi rendszer kiépítése költséges. A végrehajtási utasításokban több évig kitolták a fizikai védelem kiépítésének végső határidejét, hogy a honvédség szűkös költségvetéséből megteremthessék a törvény által előírt, elsősorban fizikai biztonsági feltételeket.

Végeredményben a szabályozás több szempontból is előnyös. Egyrészt megszűnt a nemzeti és külföldi minősített adatok kezelésének eltérő szabályozása, amely sok tévesztésre adott lehetőséget, másrészt a nemzeti minősített adataink a korábbinál sokkal nagyobb biztonságba kerültek mind fizikailag, mind egyéb betartandó rendszabályok tekintetében.

A 2009. évi CLV. számú törvény rendelkezik a minősített adat megismerésére, felhasználására, átadására vonatkozó szabályokról, az adatok felhasználásának személyi feltételeiről.

A törvény megnevezi a minősített adatok védelméért felelős szervezeteket és személyeket. Egyértelműen kimondja, hogy a Nemzeti Biztonsági Felügyelet (NBF) feladata a minősített adat védelmének hatósági felügyelete, a minősített adatok kezelésének hatósági engedélyezése és felügyelete, valamint a nemzeti iparbiztonsági hatósági feladatok ellátása.(20. § (1))

Ezzel a rendelkezés egyértelműen kimondja, hogy egyetlen hatóság, a Nemzeti Biztonsági Felügyelet (NBF) joga és kötelessége az ország területén minden minősített információ tárolása, kezelése, felhasználása engedélyezése és felügyelete.

A 90/2010. (III. 26.) Korm. Rendelet [15] foglalkozik a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről. Nagy részletességgel leírja a minősített adat kezelésével kapcsolatos személyi, fizikai biztonsági feltételeket, az adminisztratív rendszabályokat. A rendelet annyira részletes és könnyen olvasható, hogy a végrehajtó állomány munkáját nagyban elősegíti, az egyértelműen megfogalmazott pontok külön magyarázat nélkül felhasználhatóak a minősített adat kezelési folyamat előírások szerinti működtetéséhez. A szabályozás kifejezetten az adatkezelés helyszínére és körülményeire koncentrál, nem foglalkozik az adatok elektronikus feldolgozásának problémakörével. A kormányrendeletben előírt szabályok betartásával minősített adatra vonatkozó adatkezelési engedélyt kaphatunk, amely nem foglalja magában az adatok elektronikus feldolgozását.

A minősített adat elektronikus biztonságának, (valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének) részletes szabályairól a 161/2010. (V. 6.) Korm. Rendelet [16] rendelkezik. A rendelet leírja, milyen feltételeket kell teljesíteni, amikor minősített elektronikus adatkezelő rendszert, például számítógépet vagy több számítógépből álló informatikai hálózatot kell kiépíteni, akkreditálni, üzemeltetni, karbantartani. Az informatikai rendszer teljes életciklusára vonatkozó szabályrendszert tartalmaz. Nagy részletességgel leírja a minősített elektronikus adatkezelő rendszerek üzemeltetésének szabályait, kitér az üzemeltető állomány összetételére, a velük szemben támasztott követelményekre. Nagyon fontos és jól használható rendelet, mely közvetlenül a végrehajtó állomány munkáját is nagyban elősegíti.

3. KÖVETKEZTETÉSEK

A katonai nyílt adatkezelő rendszerek üzemeltetéséhez szükséges jogszabályi háttér rendelkezésre áll, ezen a területen is növelhető az elektronikai adatkezelő rendszerek kapacitása nem katonai adatkezelő rendszerek, pl. internet igénybevételével, természetesen a szükséges védelmi rendszabályok és eljárások alkalmazásával. A rendszerekben kezelt adatok hozzáférhetősége nincs szigorúan szabályozva, a rendszer elemei csatlakozhatnak nem katonai célú infokommunikációs hálózatokhoz is, ha a rendszer üzemeltetése más módon nem oldható meg. Javaslom ennek a területnek a további vizsgálatát.

A katonai minősített elektronikai adatkezelő rendszerek üzemeltetéséhez, a minősített adatok kezeléséhez a jogszabályi háttér rendelkezésre áll. Véleményem szerint a minősített információk nem katonai elektronikai adatkezelő rendszeren történő továbbításának a megvalósításával, üzemeltetési szabályrendszer kidolgozásával a hírrendszerek manőverező képessége fokozható az adatbiztonság fenntartása mellett. Ez a terület nem kiforrott, jogszabályi és hardver-szoftver elemek kialakítása szükséges az adatkezelő rendszerek összekapcsolásához. Javaslom a terület további vizsgálatát.

IRODALOMJEGYZÉK

[1] *Kivonatos lenyomat a Csendőrségi Lapok 1943. évi 3-6 számaiból.* Országgyűlés könyvtára 613/1944 sz köteles példánya. http://csendor.com/konyvtar/konyvek/Radio/R%E1dio.pdf (A letöltés dátuma: 2015. 10. 20.)

[2] Munk S.: Katonai informatika a XXI század elején. Zrínyi kiadó, 2007

[3] Kassai K.: A Magyar Honvédség információvédelmének – mint a biztonság részének feladatrendszere. Zrínyi Miklós Nemzetvédelmi Egyetem, 2007. (PhD értekezés)

[4] Haig Zs.: Az információbiztonság komplex értelmezése. Hadmérnök, Különszám (2007. 11. 07.)

[5] Muha L., Krasznay Cs.: *Az elektronikus információs rendszerek biztonságának menedzselése*. Nemzeti Közszolgálati Egyetem, 2014.

[6] AAP-31(A), NATO Glossary of Communication and Information Systems Terms and Definitions XLIII fejezet (45. / 116. oldal)

[7] 2009 évi CLV törvény a minősített adat védelméről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0900155.TV (A letöltés dátuma: 2016.04.16.)

[8] http://www.mszt.hu/web/guest/informaciobiztonsag1 letöltés időpontja 2016.04.15

[9] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról. http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2009/18.pdf [1517] (A letöltés dátuma: 2016. 04. 15.)

[10] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról. 15. § (1)

[11] 3/2012. (I. 13.) HM utasítás honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról.

[12] 2009 évi CLV törvény a minősített adat védelméről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0900155.TV (A letöltés dátuma: 2016.04.16)

[13] TEMPEST: Speciális árnyékolástechnikai követelmények (NATO SDIP-27/x) szerint tervezett, gyártott és nemzeti biztonsági hatóságok tanúsítványával ellátott csökkentett kisugárzású, un. TEMPEST Level A, B, C minősítésű eszközök alkalmazása. http://www.nbf.hu/tempestmer.html (A letöltés dátuma: 2016.04.16.)
[14] Security within the North Atlantic Treaty Organisation (NATO). C-M(2002)49. North Atlantic Council, 2002
[15] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1000090.KOR (A letöltés dátuma: 2016. 04. 16.)
[16] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1000161.KOR (A letöltés dátuma: 2015. 10. 20.)