HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 2. szám

SÜTŐ ÁKOS[1]

Robotzsaru (NEO) Integrált ügyviteli és ügyfeldolgozó rendszer információvédelmi lehetőségei

Robocop (NEO) as a system of integrant managemant and case process information protection possibilities

Absztrakt

A szerző a cikkben bemutatja, hogy az információs rendszerek használata az informatikai környezet drámai módon történő változásával hogyan változott meg. E folyamatos változások jelentős előnyöket kínálnak, ugyanakkor megkövetelik a rendészeti szervektől és egyéni felhasználóktól, akik az információs rendszereket fejlesztik, biztosítják, szolgáltatásaikat szervezik és felhasználják, hogy sokkal nagyobb hangsúlyt helyezzenek a biztonságra.

A szerző a cikkben bemutatja az olvasó számára a rendőrség területén használatos integrált rendszert, annak az információs műveletekkel való analógiáit és azok viszonyrendszerét is, így adva egy kis összevetést a két teljesen különböző terület kapcsolódási pontjaival.

A cikkben a szerző foglalkozni kíván általánosságban véve az információs műveletekkel, kiemelve azon belül a számítógép-hálózati védelmet, majd összeveti a rendőrségen belül használt robotzsaru rendszerrel és annak képességeivel.

A Robotzsaru rendszerrel összefüggésben kívánja a szerző elemezni azt, hogy az milyen fenyegetéseknek van kitéve – különös figyelemmel különleges jogrend esetén –, illetve ezekre milyen védelmi megoldások léteznek. Ismertetni kívánja az olvasóval azt, hogy az információs rendszerek közti összefüggés a biztonságos működtetésben található meg a rendszerek közti kapcsolatként.

Kulcsszavak: Különleges jogrend, információs műveletek, információ biztonság, integrált rendszerek

Abstract

The author in his article presents how to have became critically way the uses of the information systems with the informations climate. These usually changes

[1] c. r. százados, Borsod-Abaúj-Zemplén Megyei Rendőr-főkapitányság, Borsod-Abaúj-Zemplén County Police, E-mail: suto.akos@freemail.hu, ORCID:

offers significant preferences, however requires to police department and the single users, those develop, grant and the services organize, use to focus more safety.

The author in his article presents for the reader that the integrant system used in Police, and those system's analogy with the information operation and those relationships with each other as well, so it givens a little comparison with two completely different area's interfaces.

In the article the author usually wishes to deal with the information operations, highlighting in it the computer system's protection, than compares is with robocop system and it's abilties that uses in Police.

The author wish in cojunction the Robocop system to analyzed, what threats to be exposed – special attention with special rule of law – and to these what solution of protection is exist. I would like to describe with the readers that the context of information systems is found in safe operation, as a link between systems.

Keywords: special rule of law, information operations, information safety, integrant systems

BEVEZETÉS

Az informatika térhódítása, a számítógépek megjelenése és ezek jóvoltából létrejövő információs rendszerek kialakulása, valamint azok egy országos hálózatba történő kapcsolása, az adatok ezen a felületen való kezelése, feldolgozása és használata jelentős mértékben megváltoztatta a rendészeti, bűnügyi és egyéb szolgálatok tevékenységét is.

Az említett szolgálatok munkájának koordinálása, tervezése, szervezése, vezetése és irányítása, valamint adatfeldolgozói és adatbeviteli rendszere már teljesen más alapokon nyugszanak, mint korábban a gépírói tevékenység korszakában.

Az informatikai előrehaladással kiemelkedően magas szintre emelhető a szakfeladatok összehangolása, koordinálása és foganatosítása, mellyel elősegítésre kerülnek az általános rendőrségi feladatokat ellátó szervek Alaptörvényben és a rendőrségi törvényben rögzített alapvető feladatainak ellátása, hatékony elvégzése.

Az újnak számító fejlesztések természetszerűleg itt is, ugyanúgy mint a katonai dimenzióban magával hozták ezen rendszerek támadhatóságát és védelmének problémáját is.

Feltevésem az, hogy nem minden esetre vannak kidolgozott használati és gyakorlati útmutatások és ezek hiányában csak a rendelkezésre álló jogi szabályozók és azok alapján foganatosított béke időszakbeli rendészeti feladatok elvégzése útján lehet következtetni a rendszer különleges jogrendi működésének előnyeire és hátrányaira.

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 2. szám

INFORMÁCIÓS MŰVELETEK

A számítógépek elterjedésével és különösen azok hálózatba kapcsolásával nagymértékben megnőtt a vezetési és információs rendszerekhez való hozzáférés lehetősége, és ezzel egy teljesen újfajta támadási mód is kialakult. Az Internet ezt a tendenciát csak még jobban felerősítette. Ma már szinte valamennyi nagyobb hálózat kapcsolódik az Internethez, igénybe veszi annak szolgáltatásait. Az Internet felől azonban fel kell készülni az esetleges támadásokra is.

A védelmi szektorban az információt két területen alkalmazzák. Egyrészt az információt, mint a vezetés eszközét használják fel a hadviselésben, másrészt az információt, mint „fegyvert" alkalmazzák az információs műveletekben.[2]

„Az információs műveletek a döntéshozókat befolyásoló, politikai és katonai célkitűzések megvalósítását támogató tevékenységek, amelyek más felek információi, információs folyamatai, vezetési (C2), híradó és informatikai (CIS) rendszerei befolyásolására, ugyanakkor a saját információk és információs rendszerek felhasználására és védelmére irányulnak."[3]

Az információs műveletek célja az információs fölény, információs uralom és végső soron a vezetési fölény kivívása, a saját oldali vezetési ciklus számára időcsökkentés, a szembenálló fél vezetési időciklusa tekintetében pedig időnövelés elérése érdekében és ezek által a hadműveleti fölény elérésének elősegítése.[4]

Az információs műveletek és az információs hadviselés vonatkozásában alapvetően megállapítható, hogy tartalmában ugyanazon tevékenységet jelentik. Eltérés pusztán abban van, hogy az információs műveletek tágabban értelmezett fogalom, mint az információs hadviselés és szorosabban kötődik a katonai tevékenységekhez. A másik megkülönböztető tényező, hogy az információs hadviselést az információs társadalomban folytatott mindennemű olyan információs folyamatra értelmezik, amely a társadalom működésével kapcsolatban áll.

Az információs hadviselés keretében különböző, egymással szoros műveleti kapcsolatban lévő tevékenységeket, elemeket integrálnak és alkalmaznak. Ezen elemek mindegyike egyaránt fontos szerepet játszik az információs fölény kivívásában, megtartásában és az információs uralommá alakításában. Az elemek közt szoros kapcsolatok és összefüggések állnak fenn és a végrehajtás szintjében egymásba átnyúlnak, átfedik egymást.

Ezek a következők:

- megtévesztés;
- pszichológiai műveletek;
- műveleti-működési-biztonság;
- elektronikai hadviselés;

---

[2] http://uni-nke.hu/downloads/bsz/bszemle2006/1/06_Haig_Zsolt.pdf letöltés ideje: 2015. december 21.
[3] AJP–01(B) Allied Joint Doctrine. Ratification Draft 1. – 14–1. o.
[4] Haig, Zsolt: Network-Centric Warefare and Sensor Fusion. AARMS Volume 2, Issue 2. MZNDU, Budapest, 2003.

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 2. szám

— fizikai pusztítás, rombolás, rongálás;
— számítógép-hálózati hadviselés.

A fent megjelölt elemekről elmondható, hogy mind támadó-, mind a védelmi információs hadviselésben alkalmazásra kerülnek, azok közt éles határok nem húzhatók, hogy melyek alkalmazhatók támadó és melyek védelmi tevékenységben.[5]

ALAPTÖRVÉNY SZELLEMÉBEN A RENDÉSZETI TEVÉKENYSÉG ÚJ KIHÍVÁSAI

Magyarországon hatályba lépett Alaptörvényének szellemében kialakításra került az államszervezet hatalmi ágainak jog- és hatásköreinek újraelosztása, a közigazgatás szervezet- és feladatrendszerének, igazgatási jogosítványainak, jog- és hatásköreinek kizárólag jogszabályokon alapuló újraszabályozása, úgy normál időszaki jogrendben, mint a különleges jogrend alkalmazása során is.

A különleges jogrend bevezetésének szabályozása kötött, abban az összes időszaknak megvan a konkrét definiálása is egyaránt. Napjainkban a katasztrófaveszély, valamint ez alapján kihirdetett veszélyhelyzet kihirdetése a leggyakoribb, azonban a békeidőszaki felkészülés keretein belül fontos, hogy az összes többi időszakra történő felkészülés is megfelelő módon megtörténjen, hiszen az utóbbi hónapok, évek során lezajlott események is ezt támasztják alá.

A különleges jogrendbe tartozik a rendkívüli állapot, szükségállapot, megelőző védelmi helyzet, váratlan támadás és veszélyhelyzet, továbbá definiálták azt az időszakot is, amely esetében nem szükséges a különleges jogrend egyikének sem a kihirdetése, azonban az intézkedés elengedhetetlenné válik. Ezt „küszöb alatti" időszaknak nevezzük, és jelenleg a katasztrófaveszély nevet viseli.

Az Alaptörvény ismeretében, figyelemmel az ország védelem komplex rendszerére mind a közrend-, közbiztonság-, hadügy és a katasztrófavédelem is nemzeti ügy lett.

A NATO 2010. évi lisszaboni csúcsértekezletén elfogadott „átfogó megközelítés" elvéből adódóan a rendőrség tevékenysége is egyre komplexebbé vált, melyből fakadóan – kiemelten a különleges jogrend időszakában – igényli a védelmi igazgatási szervekkel való együttműködést, valamint annak eredményességét.[6]

Az átfogó megközelítés elve az eredményességen alapuló együttműködésen túl arról is tanúskodik számomra, hogy a rendészeti területen a rendőrségi feladatok ellátása egyfajta műveletként is tekinthetőek, melyre kellő alapot ad számomra ez a megközelítési forma. Ekként levezetve pedig a rendőri műveletek, a katonai hadviselés keretén belül foganatosított műveletekkel – az információs műveletekkel is – hasonlóságok alakulhatnak ki.

[5] Muha Lajos: Az informatikai biztonság kézikönyve 3. rész 6.3 fejezet Budapest, 2007.
[6] Baán, Mihály–Bors, István–Csiffáry, Tamás–Hári, László-Kocsis, Lajos–Szentes, László: Védelmi Igazgatás, Hagyomány és Megújulás - Magyarország Védelmi Igazgatása a Közigazgatás Új Környezetében. Egyetemi Jegyzet, Zrínyi Kiadó, Budapest, 2014.

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 2. szám

A különleges jogrendi állapot, mint béke időszakon túli úgynevezett válsághelyzet idején pedig a Rendőrségnek, mint fegyveres rendvédelmi szervnek a normálállapottól jelentősen nem eltérő rendészeti feladatokat kell ellátnia. A feladatok ellátása során nyilvánvalóan a kialakult helyzettől függően a hatóságnak komolyabb kihívásoknak kell megfelelnie magasabb szintű források és ellátás mellett. Azon túl, hogy a Rendőrség ilyenkor a katonai műveletek ellátásához hasonló ellátmánnyal, forrásokkal és logisztikával rendelkezhet, alapjaiban véve a normál-békeidőhöz hasonló módon, feladat ellátási rend alapján látja el új típusú feladatait.

A fentiek szerinti feladatok ellátását, azzal járó adminisztrációs kötelezettségeket a rendőrség a rendelkezésre álló informatikai rendszerek, így a RZS (NEO) Integrált ügyviteli és feldolgozói rendszer alkalmazásával, használatával látja el.

A rendőrség működését különleges jogrend bevezetésekor az alábbi utasítások határozzák meg legfőképpen.

A 26/2012. (VI.15.) BM utasítás a Belügyminisztérium, és a Belügyminiszter által irányított szervek készenlétbe helyezéséről, a különleges jogrend bevezetésére történő felkészülés szabályairól, valamint személyi állományának értesítéséről.

Az utasítás a Belügyminisztérium hivatali egységeire, szerveire, valamint a Belügyminiszter által irányított önálló belügyi szervekre terjed ki. Meghatározza, hogy a különleges jogrendre hogyan, milyen módon kell a BM szerveknek felkészülni, valamint meghatározza a különböző készenléti fokozatokat, az értesítés, bevonulás rendjét is.

Erre épül rá és határozza meg az ágazat ide vonatkozó rendelkezéseit, a 30/2013. (VII. 5.) ORFK utasítás az általános rendőrségi feladatok ellátására létrehozott szerv készenlétbe helyezéséről, a különleges jogrend bevezetésére történő felkészülésének szabályairól, valamint személyi állományának értesítéséről.

Az említett utasításokból kiemelném a következő fogalmi meghatározásokat.

„Készenlét: a rendőri szervek olyan állapota, mely biztosítja békeidőszakban, valamint a különleges jogrend időszakában jelentkező rendkívüli feladatok szervezett megkezdését, majd a személyi és anyagi-technikai feltételek megteremtése után a folyamatos végrehajtást.

Készenlét fokozása: olyan rendszabályok bevezetése, végrehajtása, melyek eredményeként a rendőri szervek felkészültsége egyre jobban megközelíti, illetve eléri az általánostól eltérő, a különleges jogrend időszakában jelentkező feladatok végrehajtásához szükséges szintet.”[7]

A cikkem vonatkozásban megemlíteném, hogy ezen állapotok alkalmával nagyon fontos parancsnoki teendő a mindennapos feladatok ellátása során a Robotzsaru (NEO) Integrált ügyviteli és ügyfeldolgozó rendszerben történő szolgálatvezénylés naprakész veze-

[7] 30/2013. (VII. 5.) ORFK Utasítása - az általános rendőrségi feladatok ellátására létrehozott szerv készenlétbe helyezéséről, a különleges jogrend bevezetésére történő felkészülésének szabályairól, valamint személyi állományának értesítéséről.

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 2. szám

tése, továbbá a harcérték jelentés pontos leadása is, melyet ezen rendszerben rögzítve kell leadni és továbbítani a Tevékenységirányítási Központ felé.

A jelentésben ugyanis pontos adatok kerülnek rögzítésre, hogy a következő napon kik és hányan lesznek szolgálatban (kitérve arra, hogy ki lát el közterületen szolgálatot, és ki nem), hány személy van betegállományban, gyes-en, szabadságon, illetve egyéb okból távol, külön pontban szerepelnek azon dolgozók is, akik nem rendelhetőek be. A harcérték pontos leadása azért fontos, mert amennyiben készenlét elrendelésére kerül sor, ez alapján értesítik ki a berendelni kívánt állományt.

Minden rendőri szervnél van kiértesítési terv, melyben a kapitányság teljes állományának kiértesítési adatai szerepelnek, ebben név, cím, telefonszám. A tervben foglaltak szerint, amennyiben riadóra kerül sor, a lehető leghamarabb be kell vonulni a szolgálati helyre és jelentkezni az állomány illetékes parancsnoknál a feladatok ellátása érdekben.

A készenlét fokozása, a különleges jogrend időszakában történő működés szabályai szerint a rendőri szervek a különleges jogrend időszakában jelentkező kötelezettségeik és feladataik végrehajtásának feltételeit a készenlétük fokozásával teremtik meg. Ennek során a honvédelmi célból igényelt és a Magyar Honvédség Hadkiegészítési és Központi Nyilvántartó Parancsnokság által részükre biztosított technikai eszközöket, gazdasági, illetve anyagi szolgáltatásokat veszik igénybe.

A rendőri szervek a készenlét fokozása során a jogszabályokban, a közjogi szervezetszabályozó eszközökben, valamint egyéb normákban, szervezeti és működési szabályzataikban vagy ügyrendjeikben meghatározott feladatrendszerükkel összhangban vesznek részt a honvédelmi feladatok végrehajtásában.

A fentiekben kiragadott és különleges jogrend esetén is használatos rendben elengedhetetlenül fontos az információs rendszerek – ideértve az RZS (Neo) rendszer – biztonságának megléte, általuk nyújtott szolgáltatások biztosításának folytonossága is.

Mindezek által a rendszereknek mind a készenlét idején, mind fokozott készenlét esetén is a magasabb szinten megvalósuló rendőrségi műveletekben megjelenő kihívásoknak kell megfelelniük. Azon oknál fogva, hogy a rendszerek külső-, vagy belső fenyegetések hatására vagy annak következtében manipulálva a műveletek eredményes végrehajtását nem teszik lehetővé vagy veszélyeztetik azokat.

INTEGRÁLT ÜGYVITELI ÉS ÜGYFELDOLGOZÓI RENDSZER AZ INFORMÁCIÓS MŰVELETEK SZEMSZÖGÉBŐL

Az információbiztonságot és az informatikai biztonságot gyakran összekeverik egymással. Az információbiztonság és az informatikai biztonság különbözik egymástól. Az információbiztonság a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik. Ezzel szemben például az informatikai biztonság csak az informatikai rendszerekben kezelt adatok, és az azt kezelő rendszer védelmét jelenti.

Informatikai rendszer az adatok kezelésére használt elektronikus eszközök, eljárások, valamint az ezeket kiszolgáló és a felhasználó személyek együttese. Adatkezelés az adatok gyűjtése, felvétele, tárolása, feldolgozása (megváltoztatása, átalakítása, összegzése, elemzése stb.), továbbítása, törlése, hasznosítása (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozása.

Ezek alapján az informatikai rendszerekhez tartoznak a számítástechnikai rendszerek és hálózatok, a vezetékes- mobil- rádiós és műholdas távközlés, a vezetékes- a rádiófrekvenciás és műholdas műsorszórás, a rádiós vagy műholdas navigáció, az automatizálási-vezérlési és ellenőrzési rendszerek, valamint a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.[8]

A Robotzsaru-2000 integrált ügyviteli és ügyfeldolgozó rendszer részletes elemzését követően elkezdődött egy új alapokon nyugvó, de a régi rendszer fejlesztési, működtetési tapasztalatait hasznosító kliens-szerver architektúrájú rendszer fejlesztése. A korábbi rendszer felhasználói funkcióit új logikai, illetve fizikai architektúrára helyezi a Robotzsaru NEO, és olyan új felhasználói, adminisztrációs funkciókkal bővül, melyeket a Robotzsaru-2000 rendszerben nem lehetett megvalósítani.

Alapfilozófiája, hogy a különféle adatok keletkezési helyükön kerüljenek be a rendszerbe, így elkerülhetők az időt és figyelmet igénylő utólagos adatbeviteli munkafázisok. Egyre több szakterület munkáját támogatja, azonban figyelembe kell venni, hogy az egymásra épülő folyamatokban megjelenő adminisztrációs kötelezettségek akkor csökkennek, ha minden érintett felhasználó a rendszeren belül végzi munkáját.

Az új programmal lehetőség nyílik a rendőrségen fejlődő hardver-környezet kihasználására, illetve az újabb technikai eszközök támogatására, ezáltal egyszerűen és olcsón a rendszerbe illeszthető azon szervek munkája is, akiknek nem megfelelő az elektronikus kapcsolata a számítógépes hálózatokkal.

Az alkalmazás lehetőséget biztosít más intézmények rendszerével történő együttműködésre is. Ilyen például a banki riasztó rendszer, amely a különböző pénzintézetektől érkezett riasztások azonnali kezelését, feldolgozását, az azonnali intézkedések foganatosítását támogatja.[9]

A Robotzsaru rendszer és egyéb informatikai rendszerek kapcsolata

A Robotzsaru rendszer adattovábbítási célú kapcsolatai:

a) Kriminalisztikai Archiváló Rendszer (KAR),
b) Automatikus Arcképfelismerő és Azonosító Rendszer (3AR),
c) Körözési Információs Rendszer (HERMON),
d) Bűnügyi Nyilvántartási Rendszer,
e) Központi Szabálysértési Nyilvántartó Rendszer,

[8] http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/4/10_Muha_Lajos.pdf 139-140. old. Letöltés ideje: 2016.01.20

[9] Bihonné Király, Edit: Robotzsaru NEO rendszer felhasználói kézikönyv. 24/2006. BM-IHM-NKÖM együttes rendelete alapján Robotzsaru NEO rendszer Tanúsítása, Nyíregyháza, 2014.

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 2. szám

f) Bűnügyi és Rendészeti Biometrikus Adatok Nyilvántartása,
g) SZBEKK felé a szervezett bűnözéssel összefüggő bűncselekmények vonatkozásában,
h) Központi Bírság Nyilvántartó (Nemzeti Közlekedési Hatóság),
i) Közlekedési előéleti pontot nyilvántartó szerv (KEKKH),
j) Közúti személyi sérüléses közlekedési balesetek (KSH).

A Robotzsaru rendszer on-line módon adatokat kér:

k) a polgárok személyi adatainak és lakcímének nyilvántartásából,
l) a járműnyilvántartásból,
m) a központi szabálysértési nyilvántartásból, központi okmány nyilvántartóból,
n) a HERMON Körözési Információs Rendszeren keresztül a SIS rendszerből,
o) az OIT Hivatala Gondnokoltak Elektronikus Nyilvántartásából,
p) Központi Bírság Nyilvántartótól (Nemzeti Közlekedési Hatóság).[10]

Robotzsaru rendszer a rendőri szervek alap informatikai rendszere, olyan informatikai alkalmazások együttese, amely egységes rendszerbe foglal valamennyi nyílt rendőrségi tevékenységgel kapcsolatban keletkező, illetve beszerzett elektronikus adatot és iratot. A rendőri munka jellegéhez, illetve az egyes felhasználói csoportok feladat- és munkaköréhez igazodó felhasználói jogosultságok biztosításával komplex módon támogatja a rendőri szervek munkáját az elektronikus iratkezelésen, adatszolgáltatáson és feldolgozáson keresztül. Részét képezi a Dokumentumtár, a Netzsaru rendszer és a Robotzsaru NEO rendszer.

Robotzsaru rendszer fejlesztéséért és üzemeltetéséért felelős szervezeti elem az ORFK Gazdasági Főigazgatóság Informatikai Főosztály irányításával az ORFK Fejlesztési Osztály és az ORFK Gazdasági Főigazgatóság Gazdasági Ellátó Igazgatóság Országos Helpdesk, amely a Robotzsaru rendszert fejleszti és üzemelteti a rendőri szervek részére.[11]

A program legfőbb jellemzőit tekintve elmondható, hogy a NEO architektúrája szempontjából egy kliens-szerver üzemmódú alkalmazás. A szerver oldalon UNIX vagy LINUX operációs rendszerű központi gépeken régiós ORACLE adatbázis szolgálja ki adatokkal a munkaállomásokon futó klienseket. Valamint egy központi UNIX vagy LINUX operációs rendszerű központi gép biztosítja az országosan együttes információáramlást a szervezeti egységek között.

[10] 18/2011. (IX.23.) ORFK utasítása a Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejlesztés előírásairól

[11] 18/2011. (IX. 23.) ORFK utasítása a Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejlesztés előírásairól.

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 2. szám

A rendszer támogatja az offline-működést, amely azt jelenti, hogy csak bizonyos időközönként igényel hálózati kapcsolatot a NEO kliens. A munkaállomáson offline módban is elérhetők a lényegesebb funkciók.[12]

Az egyik legfontosabb rendszer tervezési alapelv a stabilitás volt. Minden megvalósításra kerülő funkció esetében felkészül a rendszer a tipikusnak tekinthető, szoftveres-, illetve hardveres eredetű (például hálózat) kivételek kezelésére. Az éppen munka alatt lévő helyi adatbázist, irat- és fényképtárat titkosítva tárolja.

Hely, idő, platform és kommunikáció független rendszer, azaz bármely jogosult felhasználó a rendőrség bármely a minimális hardware követelményeknek megfelelő számítógépén bármikor el tudja végezni minden iratkezelési munkáját, és azt kommunikáció megléte esetén automatikusan visszajuttatni a közös adatbázisba.

A felhasználók a megfelelő jogosultság birtokában kereséseket tudnak futtatni a nyilvántartásokban a megfelelő adatrögzítő felületekből kiindulva. A keresésekhez külön felületet is biztosít a program, ahol akár egyszerre több nyilvántartásba is elküldhetők a kérdések. A Netzsaru országos információs rendszer adatbázisában is képes kereséseket futtatni az alkalmazás. A kérdéseket egy központi szerveren futó alkalmazás dolgozza fel, s továbbítja az országos adatbázis irányába.

A felhasználók számára az információközlést egy kliens alkalmazás végzi, tehát felületet biztosít az összes elérhető információs rendszerhez. A kliens program használatával a felhasználó bárhol az országban, bármelyik munkaállomásról be tud jelentkezni, és a saját munkában dolgozni akkor is, ha azokat a munkákat az ország egy másik pontján kezdte el.

Robotzsaru NEO rendszer beépített postázási funkcióval rendelkezik, amely lehetővé teszi a munkaállomások közötti kommunikációt. A postázott csomag tartalma gyakorlatilag bármilyen olyan információ lehet, amely a párhuzamos, illetve a csoportos munkát segíti. Minden korábbi irat gyorsan hozzáférhető és teljesen vagy részben beemelhető a NEO-ban előállított iratokba.

ROBOTZSARU RENDSZER SZÁMÍTÓGÉP-HÁLÓZATVÉDELEMI ASPEKTUSBÓL

A számítógép hálózatok védelmének megvalósítása lehet passzív és aktív. A passzív védelmi módszerek és eszközök lehetnek a tűzfalak, a vírusirtók, a hozzáférés szabályozása és a behatolás detektálás és adaptív válaszlépések. Az aktív védelem módszerei közé sorolhatók a megelőző támadások, az ellentámadások és az aktív megtévesztések. [13]

Az RZS alkalmazásban az adatok védelme lényegében három szinten valósul meg. Elsődlegesen az adott felhasználót be kell illeszteni a szervezeti hierarchiának megfelelő helyére (mely főosztály, osztály, alosztály stb. tagja). Ez meghatározza, hogy mely egység

[12] Bihonné Király, Edit: Robotzsaru NEO rendszer felhasználói kézikönyv. 24/2006. BM-IHM-NKÖM együttes rendelete alapján Robotzsaru NEO rendszer Tanúsítása, Nyíregyháza, 2014.

[13] http://uni-nke.hu/downloads/bsz/bszemle2006/1/06_Haig_Zsolt.pdf, letöltés ideje: 2015. december 21. 12:10 AJP-3.10 Allied Joint Information Operations Doctrine (draft). 2002. szeptember.

anyagaihoz (ügyeihez, érkeztetéseihez, postabontásaihoz) férhet hozzá, ha azt az egyedi ügyszintű jogosultságok egyébként nem tiltják.

Ezt követően valamilyen szerepkörbe kell sorolni, amely meghatározza, hogy milyen menü-pontokat láthat, azaz milyen feladatokat hajthat végre. Ez a két szint meghatározza, hogy mely iratokhoz, ügyiratokhoz és az abban tárolt objektumokhoz férhetnek hozzá az egyes felhasználók, ezeket az adatokat a rendszergazda állítja be a felhasználó vezetőjének döntése alapján. A harmadik szintet az egyedi ügyiratszintű jogosultságok jelentik, lehetséges, hogy egy adott ügyirathoz korlátozni, esetleg kiterjeszteni akarjuk a hozzáférést.

A Rendőrség informatikai rendszereit biztonsági osztályokba kell sorolni. A védelmi intézkedések alkalmazásáért az egyes rendszereket üzemeltető informatikai szervezetek vezetői a felelősek. Az információvédelmi biztonsági osztályok:

a) Információvédelmi alapbiztonsági (1.) osztály: ide olyan adatok kerülnek rögzítésre, melyek nyíltak, jogszabályok által meghatározott és különösen nem védett adatok, például személyes, üzleti adatok.
b) Információvédelmi fokozott biztonsági (2.) osztály: ide olyan adatok kerülnek, melyek titkos, bizalmas vagy korlátozott terjesztésű minősítési szintet érnek el,
c) Információvédelmi kiemelt biztonsági (3.) osztály: pl. szigorúan titkos minősítési szintű adatok.

A rendszer tekintetében számítógép-védelmi szempontból említést érdemelnek a jelszavak használata, mint védelmi eszköz megléte. A hozzáférés szabályozás egyik leginkább alkalmazott módszere, ugyanis egy adott számítógéphez való hozzáférést sokszor kötik valamilyen jelszó használatához. Ezzel lényegében kizárható a külső beavatkozó megjelenése és csak az fér hozzá a rendszerben tárolt adatokhoz, aki azokat ismeri és megfelelően alkalmazza.

A felhasználók tekintetében kiemelendő hogy az érintett adatállományokat csak azonosított felhasználók érhetik el. Minden felhasználónak egyedi bejelentkezési azonosítóval és jelszóval kell rendelkeznie, melynek hiányában nem engedélyezett a hozzáférés. A jelszóval történő védelem esetén kiemelendő az, hogy ezeket meghatározott normák alapján kell megalkotni, nem lehetnek sablonosak, illetve meghatározott időnként azokat változtatni kell, melynek hiányában nem enged be a rendszer.

A jelszavak használatával kapcsolatban kifejthető még az, hogy egy esetleg támadás esetén – például egy jogosulatlan hozzáférő jelszó felhasználási próbálkozása – a rendszer védelmi mechanizmusokkal szükséges ellátni, mely naplózási tevékenység keretén belül valósul meg.

Ennek követelménye belső normatíva alapján meghatározott:

„Az elszámoltathatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert (biztonsági napló) kell kialakítani, mellyel utólag nyomon követhetők az informatikai rendszerben bekövetkezett -fontosabb események- különös tekintettel azokra, amelyek a rendszer biztonságát érintik és ezáltal lehetséges a hozzáférések jogosultságá-

nak ellenőrzése, illetéktelen hozzáférés megtörténtének és a felelős személyének megállapítása."[14]

Biztonságosan védett számítógép-hálózatokban gyakran többszintű jelszavas védelmet alkalmaznak, azaz egymás után több jelszókérést kell kielégíteni, ami azt jelenti, hogy a rendszerbe való belépésnél is, illetve abban futó és azzal szervesen kapcsolódó további rendszerek, így például KEKKH, körözési nyilvántartás, bűnügyi és szabálysértési nyilvántartó rendszer eléréséhez is további jelszavak kérésének kell eleget tenni. Ezen követelményeknek az RZS rendszer megfelel. A jelszavak alkalmazása sem ad azonban teljes biztonságot.

A számítógép-hálózati védelem témakörét másik aspektusból is kívánom érzékeltetni, hiszen a legtöbb esetben a védelem az információs támadásokkal szemben szoftveres úton történik leginkább, amelyre különféle víruskeresők, vírusirtók, hálózati tűzfalak, jelszavak állnak rendelkezésre.

Az idevonatkozó norma megállapítja azt, hogy:

„Minden szervezetnél ki kell alakítani azt a személyzeti struktúrát, amelynek feladata és felelőssége az informatikai rendszer megbízható üzemeltetése, ezáltal az alkalmazások megbízható működésének biztosítása. Az informatikai biztonság területén az alábbiakban meghatározott, jól elhatárolható feladatokat kell meghatározni, és az elvégzésükért felelős személyeket kell kijelölni.

Az informatikai vezetőnek ki kell jelölnie az informatikai részrendszerek, rendszerszoftverek, hálózati adatbázis-kezelők, levelező rendszerek, központi kiszolgálók, szerverek és alkalmazások rendszeradminisztrátorait, meg kell határoznia feladataikat és felelősségüket. A rendszer-adminisztrátorok és rendszergazdák feladatkörét a munkaköri leírásukban kell meghatározni. Az adminisztrátori feladatoknak összhangban kell lenniük a hardver/szoftver termék gyártója által előírt karbantartási és üzemeltetési előírásokkal.

Az informatikai vezetőnek gondoskodnia kell az üzemeltető és karbantartó személyzet olyan szintű képzéséről, hogy a hibákat mind a hardver, mind a szoftver területen képesek legyenek elhárítani, vagy a külsős szerviz partnerek részére körülhatárolni.

Rendőrség személyi állománya számára biztosítani kell a Rendőrségi informatikai rendszereinek kezeléséről, az informatikai biztonsággal kapcsolatos oktatását, vizsgáztatását."[15]

A számítógép-hálózat más hálózatoktól való elválasztásának az egyik elterjedt módja a tűzfalak használata. A tűzfalak lényegét tekintve a hálózatok közti kapcsolataként is nevezhetők, melyek közt elhelyezkedve, többek közt szűrő feladatokat látnak el. Kimondott célja akadály létesítése és ezáltal a támadás lehetőségeinek kiküszöbölése. Működésük

[14] 60/2008. (OT 32.) ORFK utasítás a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatának kiadásáról 51. pontja
[15] 60/2008. (OT 32.) ORFK utasítás a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatának kiadásáról 95-100. pontjai

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 2. szám

alapja a rendszergazdai beállítások, ugyanis nagyban függ attól, hogy milyen szűrőrendszerrel állítják be.

Említést érdemelnek az RZS rendszer vírus irtás funkcióinak megléte is, melyek különböző módszerek segítségével ismerik fel az olyan programok megjelenését, melyek ártó funkciókkal bírnak.

„Biztosítani kell a szervezet egészére, azaz a hálózat minden belépési-és végpontjára kiterjedő elektronikus vírusvédelmet. A vírusvédelmi alkalmazásnak alkalmasnak kell lennie minden fájlművelet előtt az adott fájlra vonatkozó automatikus víruskeresésre, s fertőzés esetén a fájlhozzáférés automatikus blokkolására. A vírusvédelmi alkalmazásnak alkalmasnak kell lennie valamennyi számítógépes kártevő (malware, trójai, kémprogram, tárcsázó stb.) felismerésére."[16]

Ezzel kapcsolatos feladatok ellátásért a központi menedzsment felelős, akiknek ellenőrizni kell a belépési-, és a végpontokon futó vírusvédelmi motorok hibátlan működését; a védelmi pontokon a vírusadatbázis frissességét; és a vírusincidenseket. A központi menedzsment rendszerbe be nem vont gépeket (mobil számítógépeket) egyedi vírusvédelmi alkalmazással kell ellátni. Ebben az esetben a számítógép felhasználóit ki kell képezni az alkalmazás használatára, kezelésére és ellenőrzésére, különös tekintettel a rendellenes működések felismerésére.

A számítógép-hálózati védelemről elmondható, hogy önmagában a hálózat védelmét jelenti az adatbázisokban tárolt adatok megszerzésére irányuló jogosulatlan hozzáféréssel és behatolással szemben. Ezeken kívül azonban figyelemmel kell lenni arra is, hogy a számítógép hálózatok védelmét külső szempontból is végre kell hajtani. Különös figyelemmel különleges jogrendi „hadiállapot" alkalmával megjelenő fenyegetések, veszélyek hatására nagyobb kockázat alakul ki, mint béke időszakban. Ide értjük a szándékos, erőszakos külső fenyegetéseket, melyek az információs rendszereink lerontása, avagy működésképtelenné tételére irányulnak.

Mindezen külső támadás, fenyegetés meglétének elhárítására -akár szándékos vagy katasztrófa jellegű- intézkedéseket kell tenni. Az informatikai rendszer biztonsága szempontjából azokat a helyiségeket és épületeket kell védeni, melyekben a rendszer működik. Az informatikai rendszer infrastruktúráját is ideértem, mely kiterjed az üzemeltetést végző személyzetre, illetve figyelni kell a tápfeszültség ellátásra, túlfeszültség és villám-, tűzvédelemre is egyaránt.

A védeni kívánt objektumok tekintetében különböző technológiai követelményeknek kell megfelelniük, illetve kiemelendő hogy a nap 24 órájára személyi felügyelettel kell ellátni, illetve a beléptetési rendszert is szabályozni szükséges.

[16] 60/2008. (OT 32.) ORFK utasítás a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatának kiadásáról 183-188. pontjai

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 2. szám

ÖSSZEGZÉS

Az informatikai rendszerek biztonsága nagymértékben a biztonsági előírásoktól és a helyes felhasználói magatartástól függ. A felhasználók többsége lazán kezeli a biztonsági kérdéseket, úgy gondolják eleget tudnak, vagy egyszerűen azt hiszik, hogy semmi közük nincsen az informatikai biztonság kérdéseihez. Azonban az informatika rohamos fejlődése azoktól is megköveteli a megfelelő tudást, akik nem informatikai szakterületen dolgoznak. A fenyegetések és azok veszélyeit a felhasználók ismereteinek folyamatos frissen tartásával lehet csak elhárítani.

A különleges jogrend idején foganatosítandó rendőri műveletek alapját képező rendőrségi informatikai rendszer információs műveletekkel való összehasonlítása apró betekintést engedett számomra a békeidőszaktól eltérő időben a rendőrségi működésre, kiemelve ezzel az informatikai rendszerünk előnyeit és hátrányait.

Jelenlegi állapot szerint a megfelelő informatikai tudás megszerzése a felhasználókra van bízva. A rendészeti szegmensben biztonságot veszélyeztető fenyegetésekre, nem minden esetre vannak kidolgozott gyakorlati útmutatások, tapasztalatok, ezek hiányában pedig csak a rendelkezésre álló jogi szabályozók elemzésével lehet megfelelően válaszolni, eredményezve ezzel a felhasználók informatikai biztonság tudatosságának növelését.

FELHASZNÁLT IRODALOM

1. AJP–01 (B) Allied Joint Doctrine. Ratification Draft 1. – 14–1. o.
2. AJP-3.10 Allied Joint Information Operations Doctrine (draft). 2002. szeptember.
3. Baán, Mihály–Bors, István–Csiffáry, Tamás–Hári, László-Kocsis, Lajos–Szentes, László: Védelmi Igazgatás, Hagyomány és Megújulás - Magyarország Védelmi Igazgatása a Közigazgatás Új Környezetében. Egyetemi Jegyzet, Zrínyi Kiadó, Budapest, 2014.
4. Bihonné Király, Edit: Robotzsaru NEO rendszer felhasználói kézikönyv. 24/2006. BM-IHM-NKÖM együttes rendelete alapján Robotzsaru NEO rendszer Tanúsítása, Nyíregyháza, 2014.
5. Haig Zsolt, Kovács László, Ványa László: Információs hadviselés – információs terrorizmus – kiber-terrorizmus: 6. fejezet In: Szenes K (szerk.) Az informatikai biztonság kézikönyve: informatikai biztonsági tanácsadó A-tól Z-ig. Budapest: Verlag Dashöfer Szakkiadó Kft, 2006. pp. 1-85. (ISBN:9639313122)
6. Haig, Zsolt: Network-Centric Warefare and Sensor Fusion. AARMS Volume 2, Issue 2. MZNDU, Budapest, 2003.
7. Haig Zsolt: Számítógép-hálózati hadviselés rendszere az információs műveletekben, BOLYAI SZEMLE 15. évf.:(1. sz.) pp. 54-73. (2006)
8. Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, BOLYAI SZEMLE 4. sz. pp. 137-156. (2008)
9. 60/2008. (OT 32.) ORFK utasítás a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatának kiadásáról 51., 95-100., 183-188. pontjai

10. 18/2011. (IX. 23.) ORFK utasítása a Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejlesztés előírásairól.
11. 30/2013. (VII. 5.) ORFK Utasítása - az általános rendőrségi feladatok ellátására létrehozott szerv készenlétbe helyezéséről, a különleges jogrend bevezetésére történő felkészülésének szabályairól, valamint személyi állományának értesítéséről.
12. http://uni-nke.hu/downloads/bsz/bszemle2006/1/06_Haig_Zsolt.pdf letöltés ideje: 2015. december 21. 12:10
13. http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/4/10_Muha_Lajos.pdf 139-140. old. Letöltés ideje: 2016.01.20