HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Horvayné Fehér Judit
feherjenator@gmail.com

A RENDŐRSÉG INFORMATIKAI BIZTONSÁGI STRATÉGIÁJA ALAPJAINAK MEGHATÁROZÁSA

Absztrakt

A Magyar Köztársaság Testületi Stratégiájában megfogalmazott céloknak megfelelően „a stratégia strukturálisan sajátos kettős karakterű célhierarchia: minden egyes cél úgy is felfogható, mint egy másik, magasabb rendű cél elérésének eszköze. Ez sajátos cél-eszköz piramis formájában érzékelhető, melyben a céljelleg a piramis csúcsa felé, az eszköz jelleg pedig a talapzata felé erősödik. Legfontosabb elemei a stratégiai célok, amelyek a rendőrség testületének jövőre vonatkozó legfontosabb törekvéseit foglalják össze, valamint a cselekvési sávok, amelyek a stratégiai célok megvalósításának jól körvonalazható szegmensei, amelyek az adott cél megvalósítása irányába ható, logikailag összetartozó feladatokat, feladatcsomagokat foglalnak magukba.” Ennek tükrében a rendőrség informatikai biztonsági stratégiája azon jövőbeni állapotjellemzőket kell, hogy fogalmazza meg, amelyeket a legfontosabbnak tartunk és hosszabb távon el kívánunk érni. A jelenlegi realitások között a rendőrség elé olyan középtávú célokat kell állítani az informatikai biztonság területén, amelyek egyrészt lehetővé teszik, hogy a testület a jelenlegi sok-sok gonddal küszködő „átmeneti állapotából” mielőbb kiemelkedjen, másrészt képes legyen az országnak az Európai Uniós tagságából adódó feladatok ellátására.

The strategy is a structurally special dual characterised aim-hierarchy – accordingly to the aims, stated in the Regional Strategy of the Hungarian Republic – and each aim can be conceptualized as an implement to reach another, higher aim. It can be perceived in the form of a specific aim-tool pyramid, in which the aim character strengthens into the direction of the top of the pyramid, and the tool character into the direction of the base of the pyramid. Its’ most important elements are the strategic aims, which summarize the most significant intentions of the police - in reference to the future, as well as the action-sectors, which are well-outlined segments of the realization of the strategic aims, and which conclude logically coherent tasks and task-packages – influencing the realization of concrete aims. Reflecting the above mentioned – the basic information technological security strategy for the police must formulate those future status-parameters, what we consider to be the most relevant ones and the ones we want to achieve in a long-term plan. On the base of the present reality those medium-term aims must be encountered with the police on the field of the information technological security, which can create the possibility for the police to emerge from the present-temporary state of many-many problems, and on the other hand, to make it to be able to fulfil the special tasks of the country – given by the member status of the European Union.

Kulcsszavak: *nagyobb biztonság, minőségi rendőri munka, stabil működési feltételrendszer, rendszerek megbízható üzemeltetése ~ higher security, qualitative police work, stabile working condition-system, responsible operation of the systems.*

BEVEZETÉS

Az Informatikai Biztonsági Stratégia elkészítésének célja, a rendőrségének Testületi Stratégiájában kitűzött célok eléréséhez az informatika eszközrendszerének mind hatékonyabb mozgósítása, olyan értékálló beruházások és fejlesztések eredményeként, melyek használatával javul a rendőrség reagáló képessége, növekszik a bűnelkövetők kockázatviselési kényszere, javul az állampolgárok valós biztonságérzete.

A stratégia kialakítása során figyelembe kell venni a jogszabályokban meghatározott követelményeket, a vonatkozó szabványokat és ajánlásokat, továbbá az információtechnológia fejlődéséből fakadó szempontokat.

A rendőrség informatikai stratégiájának szorosan kell kapcsolódnia a Belügyminisztérium informatikai feladataihoz, a szakirányítás eszközéül szolgáló informatikai stratégiájához. Álláspontom szerint, mindkét stratégia az informatika kiszolgáló jellegének hangsúlyozásán keresztül kíván eljutni kitűzött céljaihoz oly módon, hogy a hangsúlyt egyértelműen a szakmai (nem informatikai) vezetés által megfogalmazott feladatok kielégítésére helyezi.

A belügyminisztériumi informatikai stratégiájában megfogalmazottakat figyelembe véve az alábbi célterületeket vizsgáltam meg hogy meghatározzam a rendőrség informatikai biztonsági stratégiájának alapelveit:

- Rendvédelmi alkalmazások fejlesztése (határregisztrációs rendszer továbbfejlesztése, ujjnyomat nyilvántartó és azonosító rendszer továbbfejlesztése, egységes rendőrségi ügyfeldolgozó rendszer a Robotzsaru teljes körű kialakítása).
- Az informatikai szolgáltatási háttér rekonstrukciója (belügyi kezelésű alapnyilvántartások fejlesztése, egységes közgazdasági információs rendszer kialakítása, a választási információs rendszer, az ügyeleti rendszer továbbfejlesztése).
- Egységes hálózati infrastruktúra kialakítása (virtuális hálózatok kialakítása rendőrségi, határőrizeti, közigazgatási szolgáltatási feladatokhoz, egyenszilárdságú lokális hálózatok kialakítása, a távbeszélő szolgáltatások egységes, digitális szintre hozása, a ”112” hívószám használati feltételeinek végleges kialakítása, az EDR készenléti rádió-távközlési szolgáltatás bővítése, az országos funkcionális rejtjelezett kommunikáció megvalósítása).
- Közhitelességhez kapcsolódó alkalmazások kialakítása (Okmányirodák informatikai hátterének fejlesztése, a központi okmány-előállítás informatikai hátterének támogatása, az elektronikus átvitel hitelességének – biztonságának – megvalósítása).
- Közigazgatási szolgáltatások fejlesztése (Egységes címnyilvántartás kialakítása közigazgatási területi informatikai központokban, nyilvános lakossági információs rendszer korszerűsítése).

Vizsgálati körben, olyan új feladatok jelentek meg a rendőrség oldaláról (pl. a keleti határszakasz őrizetének és ellenőrzésének megerősítése, nemzeti adattár véglegesítése, a nyilvántartások adattartalmának, az adatvédelem elveinek, az elérhetőség technikai feltételeinek egységesítése), amelyek elengedhetetlenné teszik a határőrizet, a határforgalom-ellenőrzés, a menekült-, a migrációs és a bevándorlási politika és kapcsolatrendszerének, információs rendszereinek, technikai eszközeinek átértékelését. A fenti területek vizsgálatával olyan biztonsági követelményrendszert javaslok, melyet mind középtávú mind hosszú távú stratégiai célok elérésénél figyelembe kell vennünk.

A RENDŐRSÉG INFORMATIKAI STRATÉGIAI TERVE

Az informatikai stratégia kialakítása

Stratégián a célok, valamint a célok eléréséhez szükséges eszközök és módszerek együttesét értjük. A stratégia időbeli hatályát a rendőrség feladatrendszerének, a feladatrendszeren belül a súlypontokat meghatározó vezetői akaratnak, valamint az informatikai szakma eszközrendszerének változási sebessége is meghatározza.

A rendőrség informatikai stratégiájának szakmai célja a jelenlegi rendszerek megbízható üzemeltetése, az EU csatlakozás, a Schengeni rendszer követelményei szerinti fejlesztések előkészítése, a rendőrszakmai (vezetői, beosztotti) munkát támogató alkalmazások fejlesztésének kell, hogy legyen.

A stratégiánk kialakításához meg kell határoznunk, hogy

- hol vagyunk most - Helyzetértékelés,
- hová akarunk eljutni - Célkitűzés, elvárások,
- hogyan juthatunk oda - ennek megfelelő informatikai stratégia, feladatok meghatározása.

Ennek érdekében meg kell vizsgálnunk az *informatika kiszolgáló jellegét.* Az informatika nem cél, hanem eszköz. Az informatikai stratégiát a rendőrségnek szakmai célkitűzéseiből kell levezetnie. Érvényesíteni kell a környezeti feltételek rugalmas visszacsatolását, az interaktív szakmai tervezést, ezen belül:

- az alaptevékenységek szakmai prioritásait,
- az informatikai prioritásokat,
- a költségvetés-tervezési prioritásokat.

Az egységesség érvényesülésének elvét kell követni, hogy a fenti célkitűzések teljesüljenek.

A rendőrség a stratégiai terve kötelezően figyelembe veszi a BM által meghatározott szabványokat, ajánlásokat, egyéb előírásokat (melyek értelemszerűen tartalmazzák az Európai Unió, a NATO, valamint a nemzeti szabványokat), végrehajtja a szakmai célkitűzéseinek BM által való egyeztetését a közös elemek használása céljából más érintett szervezetek vonatkozásában. Harmonizációra törekszik a rendvédelmi és fegyveres szervekkel, illetve más államigazgatási, állami szervekkel egyaránt.

Ennek tükrében az informatikai stratégiának *egységesen kell kezelnie* az információrendszerek és alkalmazások, a számítástechnikai eszközök és a kommunikációs infrastruktúra korszerűsítésére irányuló fejlesztések tervezését és megvalósítását. Az egységességet (szabványosságot) meg kell valósítani mind az infrastrukturális, mind pedig az alkalmazásfejlesztéseknél.
Megvizsgálva a rendőrségre vonatkozó kormányhatározatokat, belügyi rendelkezéseket, azokat feldolgozva és a Közigazgatási Informatikai Bizottság (a továbbiakban: KIB), illetve a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság (a továbbiakban: MeH ITB) vonatkozó ajánlásait kell szem előtt tartani az informatika biztonsági stratégia megalkotásánál.

AZ INFORMATIKAI BIZTONSÁGI STRATÉGIA ALAPELVEINEK MEGHATÁROZÁSA

A követelményrendszer meghatározásánál feldolgoztam az ISO/IEC 27002:2005 szabványt, a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 10., 13. és 17. számú ajánlásait, továbbá a KIB 25. számú ajánlásából (Magyar Informatikai Biztonsági Ajánlás) a Magyar Informatikai Biztonsági Irányítási Követelményrendszer (MIBIK) részeit az Informatikai Biztonsági Irányítási Rendszert (IBIR), az Informatikai Biztonsági Irányítási Követelményeket (IBIK), az Informatikai Biztonsági Irányítás Vizsgálatát (IBIV), a Magyar Informatikai Biztonsági Értékelési és Tanúsítási Sémát (MIBÉTS), továbbá az ezek alkalmazását támogató KIB 28. számú ajánlást, a KIB 19. számú ajánlását, alkalmazva a COBIT 4.1 és az ITIL V3 módszereket, követelményrendszerét [1-13]. Az alábbi alapelvek érvényesülését tartom fontosnak az informatikai biztonsági stratégia megalkotása során a rendőrségnél:

- *Bizalmasság:* biztosítani kell a rendőrség kezelésében és használatában lévő adatok, információk tekintetében mind a központi, mind a helyi feldolgozások, valamint az adat- és információcsere során, „hogy az adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról”[14]
- *Sértetlenség* folyamatosan biztosítani kell a rendőrség által kezelt, feldolgozott és közzétett adatokra mind a feldolgozás, mind pedig az adat- és információcsere során.
- *Rendelkezésre állás:* biztosítani kell a külső és belső adatkérések során, hogy az adatok az „arra jogosultak által a szükséges időben és időtartamra használható”

A három alapelvet tovább vizsgálva a stratégiai célkitűzések eléréséhez a további elvek szem előtt tartását javaslom a dokumentum elkészítéséhez:

A folyamatosság elve

Figyelembe kell venni az eddig megvalósult fejlesztéseket, szervesen kell építkezni azok eredményeire. Számításba kell venni a következő tervezési ciklusra maradó feladatokat, az informatika, a számítástechnika, a távadat-átvitel várható fejlődésének irányait, a hosszabb távra terjedő rendőri feladatokat.
A megvizsgált dokumentumok értelmezésiből elfogadtam, hogy *„Az informatika az információ természetével, a vele, kapcsolatos tevékenységekkel (gyűjtésével, ábrázolásával, továbbításával, tárolásával, feldolgozásával, védelmével, megsemmisítésével stb.), e tevékenységeket megvalósító és/vagy támogató rendszerekkel, továbbá a rendszerekkel, kapcsolatos tevékenységekkel (tervezés, fejlesztés, szervezés, üzemeltetés, kiértékelés, minőségbiztosítás) foglalkozó szakág.*[15]

A rendőrség tekintetében ezek alapján, értelmezésem szerint:
Az informatika rendőrség feladatrendszerébe illesztve olyan, az alapfeladatokat hatékonyan támogatni képes eszköz, mely a számítástechnika és a kommunikáció eszközrendszereinek felületi és működési integrálásával képes a rendőri alapfeladatok támogatásán túl, a civil közigazgatás és ezen keresztül az állampolgárok felé magas szintű szolgáltatást nyújtani.

Véleményem szerint, az informatika részének kell tekinteni a távközlést is, így a továbbiakban informatikai stratégián a rendőrség távközlési és számítástechnikai szolgáltatási egységeinek közös stratégiáját értem.

A Rendőrségnek a közbiztonsági helyzet javítására, a bűnözés visszaszorítására kidolgozott hároméves középtávú fejlesztési programja (1053/1997. (V.28.) Kormány határozat) [16] a szervezet erőforrásait minden területre kiterjedően mozgósítani kívánja, és a meglévő eszközrendszer optimális felhasználásával egy átfogó szolgáltatásfejlesztési folyamatot akar beindítani. Ezen szakmai célkitűzés értelmében az emberi, tárgyi és pénzügyi erőforrások sorába fel kell venni az információt is. Ahhoz, hogy az informatikát a Magyar Rendőrség erőforrásai közé fel tudjuk venni szükség, van a szervezet globális céljait és érdekeit érvényesíteni, és a részletekkel harmonizálni tudó vezetésre, irányításra, koordinációra, szervezeti és működési rendre.

Ennek gyakorlati megvalósításaként, a fejlesztési folyamat egyik közvetlenül vezérelhető és gyors eredményeket felmutató területe lehet a közterületi rendelkezésre állás hatékonyságának növelése. Ennek elérése érdekében szükségesnek tartanám a rendőrségi alapinfrastruktúra fejlesztését, különös tekintettel az informatika és a távközlés eredményeinek és lehetőségeinek felhasználására, mellyel növelhetővé válik az informatikai biztonság is.

A fokozatos fejlődés elve

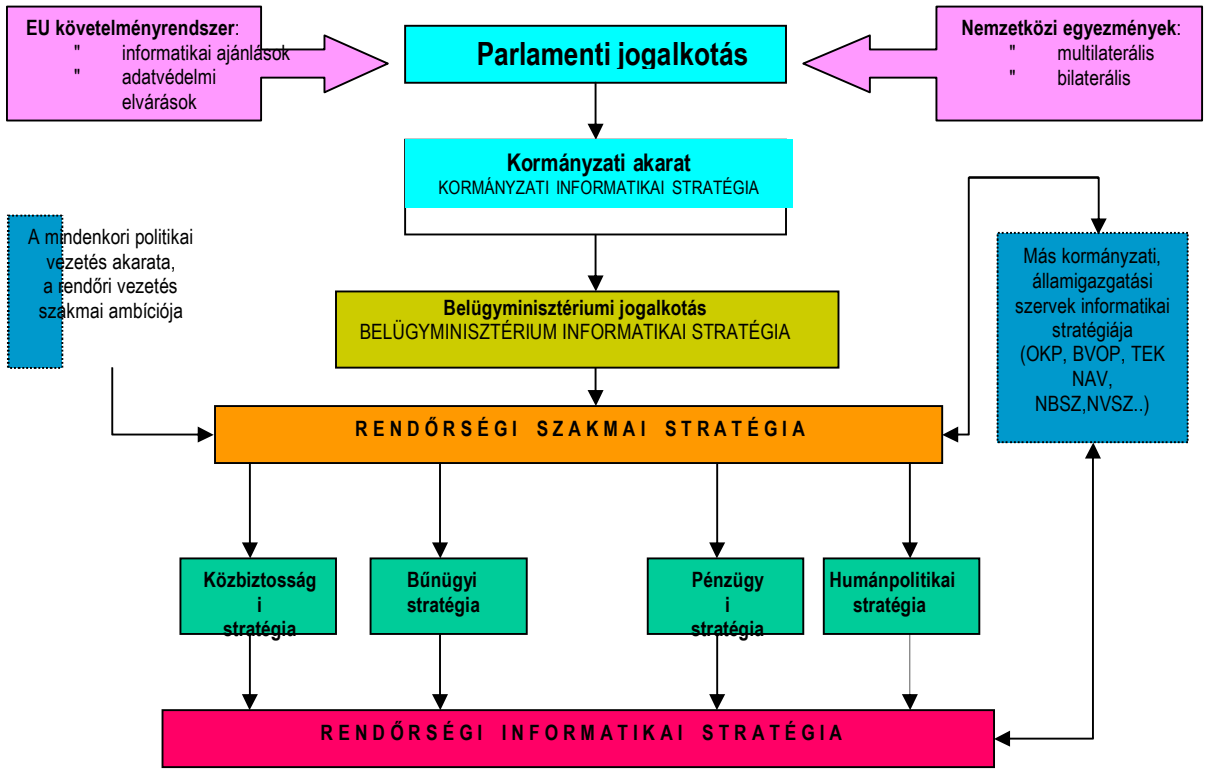
Az informatikai biztonsági stratégiának rövid helyzetértékelés alapján fel kell tudnia vázolni az informatikai alkalmazások lehetséges irányait, a rendőri munkát átfogóan támogató információrendszerek fejlesztésének és működtetésének alapelveit és rövidtávon kitűzhető céljait, valamint a megvalósítás lehetséges eszközrendszerét.
Véleményem szerint az informatikai biztonsági stratégia elfogadása és következetes megvalósítása jelentős előnyökkel jár, hisz a tervszerű rendőri munka nem nélkülözheti az informatika szolgáltatásait, másrészt az informatika mind újabb területeire hatol be a rendőri munkának, megváltoztatva és korszerűsítve az adott szakmai tevékenységet.
Jóllehet a korszerű informatikai megoldások iránti fogadókészség fokozatosan fejlődik, ma még számos területen hiányzik a vezetői elkötelezettség, a jogi keretek sem támogatják mindig ezen megoldások bevezetését. Az információ- és adatgazda szerepek, feladat-hatáskörök- és felelősségi viszonyok rendezetlenek, s ennek következtében a meglévő információrendszerek működési hatékonysága rendkívül alacsony.

A fokozatosság elvének teljesülését vizsgálva azt tapasztaltam, hogy informatikai rendszereknek a rendőrségen belül is kialakult egy jellegzetes rétegszerkezete, amelynek tipikus szintjei:

- Az univerzálisan használható, infrastruktúra jellegű hardver és alapszoftverek.
- Az erre épülő feladat-specifikus alkalmazói szoftverek.
- A szervezeti feltételeket, a szervezetbe való illeszkedést biztosító orgver, ami szabályzatokban, ügyrendekben, munkaköri leírásokban jelenik meg.
- A rendszerek teljes életciklusára kiterjedő szervezési feladatokat ellátó informatikai menedzsment.

Az állandó helyzetvizsgálat elve

Az informatika szerepe a világ minden nagy szervezeténél így a rendőrségnél is, hogy hatékonyan biztosítsa a szervezetszerű feladatok kiszolgálását a koncepcionálisan kitűzött szervezeti célok elérését. Az informatika tevékenység rendszerének helye és szerepe a rendőri tevékenységek rendszerében mindig változott.



Ahhoz, hogy tényszerű megállapításokat tegyünk, két irányt kell megvizsgálnunk a helyzetvizsgálat során: a kialakult informatikai helyzetet (Hol vagyunk most?) és az általános informatikai célkitűzéseket (Hova akarunk eljutni!)

Az első irány szerint, a rendőrség első önálló informatikai koncepciója 1991 végén, 1992 elején alakult ki. A koncepció lényegét röviden összefoglalva " 3-5 év alatt létre kell hozni az európai szintű informatikát a magyar rendőrségnél". A koncepció felső szintű elfogadását követő munkálatok elsődlegesen általános –extenzív növekedés keretében megvalósuló - modernizációs programot céloztak meg, kevésbé kötődtek konkrét rendőri szolgálati stratégiához. Ezt a koncepciót követték a többi, 5 évenként megújuló stratégia tervezetek is.

A második irány vizsgálatakor a megvalósítandó informatikai stratégia célja, a bűnügyi és közbiztonsági események jellegéből fakadóan, globális – az egész ország területére, bizonyos tekintetben az országhatárokon túlra is kiterjedő – rendőri szakmai munka támogatását célzó, a területileg és szervezetileg elszigetelt informatikai rendszerek közötti kapcsolat megteremtése, azaz egységes, országos rendőrségi információs rendszer kiépítése. A rendszer célja, hogy biztosítsa a rendőrségi alapfeladatok magasabb színvonalú ellátásához szükséges információk gyors és biztonságos áramlását, infrastruktúrát képezzen a szakmai munkát

támogató, valamint a rendőrség egészének működését biztosító globális és lokális számítástechnikai eszközök, rendszerek, alkalmazások futtatására.

Összefoglalva a két irányt: *A rendőrségi informatikai stratégia a meglévő informatikai és távadat-átviteli hálózati alapokra, a meglévő számítástechnikai eszközök és humán szakmai bázis felhasználásával egy – a rendőri alapfeladatokat támogató - szolgáltatási információs hálózat alapjait teremti meg.*

A biztonságra törekvés elve

Az informatikai biztonsági stratégia megtervezése során törekedni kell a biztonság megteremtése érdekében a további elvek érvényesítésére:

- Törvényesség garantálása.
- Hitelesség garantálása.
- Azonosítással hitelesítés.
- Elszámoltathatóság kialakítása.
- Hozzáférés-szabályozás.
- Jogosultság kiosztás és annak ellenőrzése.
- Auditálhatóság logikai védelmi funkcióinak megteremtése.
- Bizonyítékok rendszerének és folyamatának kialakítása.
- A hibákat elsősorban nem kijavítani, hanem megelőzni kell.

A rendőrség informatikai biztonságának megteremtése érdekében szabályozott formában, a stratégiában az alábbiakról kell gondoskodni:

- Az informatikai biztonság részletes követelményeinek rögzítése az informatikai biztonság dokumentációs rendszerben.
- Az informatikai biztonsággal kapcsolatos szervezeti és hatásköri kérdések, valamint a rendőrségen belüli és az azon kívüli adatkapcsolatok szabályozása.
- A rendőrség adat és információs vagyonának védelmét szolgáló minősítési és biztonság osztályba sorolási eljárás kialakítása, valamint annak ellenőrzési módja.
- A személyekhez és szerepkörökhöz kapcsolódó biztonság követelmények, az oktatási és képzési tervek, valamint biztonság események és meghibásodások esetén szükséges eljárások kialakítása.
- Az informatikai biztonsághoz kapcsolódóan az informatikai rendszerek fizikai és környezeti biztonságának kialakítása.
- Az alkalmazott üzemeltetési és kommunikációs eljárások informatikai biztonság követelményrendszerének meghatározása.
- Az informatikai eszközökhöz, adatokhoz és informatikai szolgáltatásokhoz történő hozzáférés szabályainak kialakítása és alkalmazása.
- Az informatikai rendszerfejlesztési és karbantartási eljárások létrehozása.
- Az informatikai infrastruktúra folyamatos működésének biztosítását szolgáló eljárások kialakítása.
- Az informatikai infrastruktúra, eljárások és szolgáltatások jogszabály megfelelőségét biztosító szabályozás kialakítása.
- A védelmi célkitűzések és informatikai biztonság követelmények teljesítése érdekében biztosítani kell a kellően költséghatékony, kockázatokkal arányos védelmi intézkedések és ellenőrzések – a mindenkori rendelkezésre álló erőforrásoknak megfelelő – alkalmazását.

- Az rendőrség informatikai biztonsági stratégiája, a már megfogalmazott informatikai biztonság filozófiára-politikájára kell épülnie, és megfelelő alapot kell teremtenie az informatikai biztonság célkitűzések meghatározásához.
- *Az informatikai biztonsági stratégiának minden lehetséges esetben a proaktív, azaz megelőzésre törekvő magatartást kell előnyben részesítenie a reaktív, azaz követő magatartással szemben.*
- Az informatikai biztonsági stratégiának az informatikai biztonsággal összefüggő szabályoknak, intézkedéseknek egységes értelmezését kell elősegítenie.

Az informatikai szervezetek irányítása

Az elmúlt időszakban fokozatosan kialakult egy informatikai szakszolgálat alapja, mely még nem kellően szabályozott, a munkamegosztás nincs megfelelően elhatárolva. Jórészt emiatt, a rendőrségi informatikai menedzsment számára az informatikai terület nehezen áttekinthető és kezelhető. Véleményem szerint *az eredményes informatikai tevékenység egyik alapfeltétele az informatikai szakszolgálat hivatalos létrehozása, a rendőrségi struktúrához illeszkedő tagolása, a hatáskörök és döntési folyamatok szabályozása.*

A központi, területi informatikai rendszerek megfelelő működtetéséhez megfelelő hozzáértésű rendszergazdákat kell biztosítani. Szakirányításukra többféle modell is elképzelhető, mivel mind az alkalmazó szervezet működési igényeinek, mind az informatikai szakma elvárásainak eleget kell, hogy tegyenek. Ennek tükrében két modellt választottam ki.

Az egyik modell a *központi szervezettől elvárható feladatok* körébe sorolom a rendőrség szakmai stratégiájának kidolgozásában való részvétel, majd ennek alapján az informatikai stratégia kidolgozása, éves tervekre történő lebontása, végrehajtása, karbantartása. A másik modell *az informatikai stratégiából fakadó szabványosítási feladatok ellátása* (eszközellátási szabványok, adatbázis szabványok, informatikai fejlesztési, üzemviteli, ellátási normatívák, intézkedések, utasítások kidolgozása).
Részleteiben az informatikai stratégiából fakadó rendszerfejlesztési feladatok ellátását az alábbiakban fejtem ki:

- Az informatikai stratégia megvalósítását biztosító gazdálkodási feladatok ellátása (költségvetés tervezés, költségvetéssel történő gazdálkodás, előirányzat felhasználás figyelés, kötelezettség nyilvántartás, köz- és egyéb beszerzések, szerződés nyilvántartás, eszköznyilvántartás, raktározás, stb.).
- Az informatikai stratégia eredményeként megjelenő üzemeltetési feladatok ellátása (országos rendszerek üzemeltetése, az amortizációs tevékenység ellátása, központi adatbázisokhoz való hozzáférés biztosítása, adattárakból történő szolgáltatás biztosítása, országos szerviztevékenység részleges ellátása).

Fejlesztés, koordináció, felügyelet szem előtt tartása

Az informatika stratégia megalkotásánál az informatikai fejlesztések területén a szolgálati ágak által megfogalmazott igények, és az ezek támogatására irányuló feladatok az elsődlegesek. Ezeknek az elvárásoknak való megfelelés érdekében az informatikusi szakgárdán belül ki kell alakítani az egyes szolgálati ágaknak megfelelően a szakreferensi feladatköröket, amelyek „kettős irányítással”, de az informatikai szervezeten belül látják el feladataikat. Biztosítani kell olyan informatikai képzettséggel, gyakorlattal rendelkező

szakembereket, akik szakterületek igényeit össze tudják hangolni az informatikai lehetőségekkel és a szakszolgálattal.

A biztonsági szempontokat figyelembe véve a fejlesztéseknél az előkészítő, a koordinációs feladatokra, a követelmények megfogalmazására, a késztermék átvételére erőforrást kell biztosítani. A fejlesztéseket professzionális szolgáltatást nyújtani tudó szervezetekkel kell elvégeztetni. A megfelelő színvonal gazdaságos biztosíthatóságához elsősorban a szolgáltatásvásárlást kell előnyben részesíteni, de erre specializálódott szolgáltató szervezetek kialakítása is alkalmazásra kerülhet. Ki kell alakítani az informatikai szakirányítást megalapozó modelleket, minőségbiztosítási elveket, szabályokat és ajánlásokat.

Az informatikai biztonsági stratégiai kérdésének tartom a fejlesztések során, hogy érvényesíteni kell az egységes rendszertechnika elvét. Létre kell hozni a központi adatszabványokat. A központi rendszerek vonatkozásában könnyen menedzselhető, áttekinthető jogosultsági rendszert kell kialakítani.

ÖSSZEGZÉS

Az Informatikai Biztonsági Stratégia elkészítésének célját meghatározva, a rendőrségének Testületi Stratégiájában kitűzött célok eléréséhez az informatika eszközrendszerének mind hatékonyabb mozgósítása, olyan értékálló beruházások és fejlesztések eredményeként, melyek használatával javul a rendőrség reagáló képessége, növekszik a bűnelkövetők kockázatviselési kényszere, javul az állampolgárok valós biztonságérzete.

A rendőrség informatikai stratégiájának szakmai célját a jelenlegi rendszerek megbízható üzemeltetése, az EU csatlakozás, a Schengeni rendszer követelményei szerinti fejlesztések előkészítése, a rendőrszakmai (vezetői, beosztotti) munkát támogató alkalmazások fejlesztésében állapítottam meg.
Figyelembe vettem a vizsgálat során a bizalmasság, sértetlenség, rendelkezésre állás alapelveit. Meghatároztam, hogy az informatika rendőrség feladatrendszerébe illesztve olyan, az alapfeladatokat hatékonyan támogatni képes eszköz, mely a számítástechnika és a kommunikáció eszközrendszereinek felületi és működési integrálásával képes a rendőri alapfeladatok támogatásán túl, a civil közigazgatás és ezen keresztül az állampolgárok felé magas szintű szolgáltatást nyújtani.

Rendszerbe szettem a rendőrség informatikai biztonsági stratégiájának megalkotása során alkalmazandó alapelvek sorát mely szerint:

- a folyamatosság elve:
- a fokozatos fejlődés elve
- Az informatikai biztonsági stratégiának rövid helyzetértékelés alapján fel kell tudnia vázolni az informatikai alkalmazások lehetséges irányait, a rendőri munkát átfogóan támogató információrendszerek fejlesztésének és működtetésének alapelveit és rövidtávon kitűzhető céljait, valamint a megvalósítás lehetséges eszközrendszerét.
- az állandó helyzet vizsgálat elve
- meghatároztam a rendőrségi informatikai helyét a rendőrségen belül és a kormányzaton belül
- Az iránymutatás szükségessége keretében a rendőrségi informatikai stratégia a meglévő informatikai és távadat-átviteli hálózati alapokra, a meglévő

számítástechnikai eszközök és humán szakmai bázis felhasználásával egy – a rendőri alapfeladatokat támogató - szolgáltatási információs hálózat alapjait teremti meg.

- a biztonságra törekvés elveként Az informatikai biztonsági stratégiának minden lehetséges esetben a proaktív, azaz megelőzésre törekvő magatartást kell előnyben részesítenie a reaktív, azaz követő magatartással szemben.
- az informatikai szervezetek irányítása szerint az eredményes informatikai tevékenység egyik alapfeltétele az informatikai szakszolgálat hivatalos létrehozása, a rendőrségi struktúrához illeszkedő tagolása, a hatáskörök és döntési folyamatok szabályozása.
- Fejlesztés, koordináció, felügyelet szem előtt tartása.

Összefoglalóan elmondható, hogy a rendőrség informatikai biztonsági stratégiája azon jövőbeni állapotjellemzőket kell, hogy fogalmazza meg, amelyeket a legfontosabbnak tartunk és hosszabb távon elkívánunk érni.

FELHASZNÁLT IRODALOM

[1] ISO/IEC 27002:2005 szabvány

[2] MEH ITB 10. számú ajánlás

[3] MEH ITB 13. számú ajánlás: Internet a Kormányzatban – Intranet, 1.0 verzió Budapest, 1997

[4] MEH ITB 17. számú ajánlás: Elektronikus adatcsere1.0 verzió Budapest, 1997

[5] KIB 25. számú ajánlása: Magyar Informatikai Biztonsági Irányítási Követelményrendszer (MIBIK) 1.0

[6] KIB 25. számú ajánlása: Informatikai Biztonsági Irányítási Rendszer (IBIR) 1.0

[7] KIB 25. számú ajánlása: az Informatikai Biztonsági Irányítási Követelmények (IBIK) 1.0

[8] KIB 25. számú ajánlása: Informatikai Biztonsági Irányítás Vizsgálata (IBIV) 1.0

[9] KIB 25. számú ajánlása: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)

[10] KIB 28. számú ajánlása: E-Közigazgatási Keretrendszer 1.0

[11] KIB 19. számú ajánlása: A közigazgatás szervezetei által működtetett honlapok tartalmi és formai követelményeire, verzió: 3.0

[12] COBIT (Control Objectives for Information and related Technology) "Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzések" verzió 4.1, IT Governance Institute, 2007.

[13] ITIL (IT Infrastructure Library) az informatikai szolgáltatásmenedzsment verzió: V3 2011.

[14] Muha Lajos: az informatikai biztonság egy lehetséges rendszertana, Bolyai Szemle XVII. évf. 4. szám, pp 137-156., 2008.

[15] Az Informatikai Tárcaközi Bizottság (ITB) 10.sz. ajánlásaként kiadott „ A központi államigazgatás informatikai stratégiája 1995-0997.”, INFORMATIKAI TÁRCZKÖZI BIZOTTSÁG Melléklet a kormányzati informatikai koordináció továbbfejlesztésére készített kormány-előterjesztés tervezetéhez , Budapest, 1995. http://www.itb.hu/dokumentumok/archivum/bg.html

[16] 1053/1997. (V.28.) Kormány határozat A Rendőrségnek a közbiztonsági helyzet javítására, a bűnözés visszaszorítására kidolgozott hároméves középtávú fejlesztési programja Magyar Közlöny 26.szám