MUNK SÁNDOR

AZ INFORMATIKAI BIZTONSÁG RENDSZERTANÁHOZ[1]

ON THE TAXONOMY OF INFORMATION SECURITY

Az informatikai biztonság korunk egyik megkerülhetetlen kérdése, problémája és feladata, amellyel publikációk tömege foglalkozik. A Bolyai Szemle 2008/4. számában jelent meg egy publikáció az informatikai biztonság rendszertanáról, amely jelentőségénél fogva vitára, továbbgondolásra érdemes. Sajnos a hadtudomány területén elég ritka a kutatási eredményekre közvetlenül reagáló publikáció, pedig érdemi eredmények igazán csak egymásra épülve, eszmecserék során születhetnek meg. Jelen publikáció célja az említett anyagban foglaltak elemzése, értékelése, továbbgondolása. Ennek érdekében: vizsgálja a rendszertani alapokat, a kitűzött célt és annak megvalósítási módját, valamint magát a javasolt rendszertant és megfogalmazza az ezekkel kapcsolatos észrevételeket. Kulcsszavak: informatikai biztonság, rendszertan.

Information security is one of the inevitable questions, problems and tasks of our ages, that is studied by a lot of publications. A publication appeared in the 2008/4. issue of Bolyai Szemle presenting a taxonomy of information security, that due to its significance worth to discuss, and think about. Unfortunately in the field of military sciences there are rather few, if any publications that directly respond to scientific results, although considerable results can only be reached based on another, in the process of discussions. Recent publication aims at analysing, evaluating, and extending the ideas found in the material mentioned. For this purpose: examines the taxonomical basics, the goal of the publication and the way of its realization, as well as the suggested taxonomy itself, and presents remarks, reflections. Keywords: information security, taxonomy.

Bevezetés

Korunk alapvető jellemzője az információs folyamatokat, tevékenységeket támogató technológiák eszközeinek és szolgáltatásainak folyamatosan bővülő alkalmazása, a hálózatok világméretű elterjedése, a legkülönbö-

[1] Gondolatok a Bolyai Szemle 2008/4. számában megjelent, „Az informatikai biztonság egy lehetséges rendszertana” című publikációjához [1] kapcsolódóan.

zőbb folyamatok egyre fokozódó információtechnológiai szolgáltatásfüggősége. A 'mindenütt jelenlévő' informatika korábban nem látott szolgáltatásokat nyújt, ugyanakkor új problémák megjelenésével is együtt jár. Az informatikai rendszerek és összetevők új sebezhetőségeket hordoznak, új — elsősorban információs jellegű — veszélyeztető hatások számára teremtenek lehetőségeket. A biztonság kérdéseinek szerepe, jelentősége általában és ezen belül kiemelten az informatikai rendszerek biztonságának területén folyamatosan nő.

A Bolyai Szemle 2008/4. számában jelent meg egy, a Robothadviselés 8. konferencián elhangzott előadás szerkesztett változata [1], amelyben Muha Lajos — alapvetően oktatási, oktatástervezési felhasználásra — egy informatikai biztonsági rendszertan (az előadásban még taxonómia) kialakítását célozta meg. A publikáció első felében az informatikai biztonság fogalmi alapjait elemzi, majd rövid indoklás után közread egy lehetséges (javasolt) rendszertant. A felvetett kérdéskör önmagában is, oktatási felhasználási szempontból is olyan jelentőséggel bír, ami indokolttá teszi elemzését, továbbgondolását. Sajnálatos módon a hadtudományban és a katonai műszaki tudományban rendkívül ritka a megjelent — publikált, vagy előadott — tudományos eredményekre, véleményekre történő közvetlen reagálás, ami megítélésem szerint egy szakterület tudományos életének elengedhetetlen része kell(ene) legyen. A következőkben foglaltak ezen hiányosság csökkentésére irányuló kísérletnek is tekinthetőek.

Jelen publikáció alapvető célja tehát elsősorban a hivatkozott publikációban foglalt egyes gondolatok elemzése, értékelése, továbbgondolása. Ennek érdekében:

— az elemzés megalapozásához összegzi a rendszertan, besorolástan (taxonómia) alapvető kérdéseit;
— elemzi és értékeli az informatikai biztonság rendszertanának célját, valamint megvalósításának módját;
— végül elemzi a javasolt rendszertanban foglalt tartalmat és következtetéseket fogalmaz meg a további feladatokra.

A rendszertan, taxonómia alapjai

A rendszertan és taxonómia fogalmaknak hosszú ideig konkrét, az élőlények rendszerezéséhez kapcsolódó tartalmuk, értelmezésük volt, ami mára már kibővült más dolgok, objektumok rendszerezésére is. A két foga-

lom viszonyának értelmezése sem teljesen egyértelmű, a két leggyakoribb nézet egyike szerint a két fogalom lényegében egymás szinonimájának tekinthető, a másik szerint a rendszertan a magasabb szintű, a taxonómia pedig annak egyik összetevője. A következőkben röviden összegezzük az alapvető fogalmak leggyakoribb meghatározásait.

A rendszertan (szisztematika) a Magyar Nagylexikon szerint „az élőlények élő és kihalt típusait leíró, …azokat meghatározott tud[ományos] elvek szempontjai szerint csoportokba soroló tudományág". [2, 402. o.], a besorolástan (taxonómia) pedig „a tágabban értelmezett rendszertan egyik részterülete, … szűkebb értelemben a rendszertan alapelveinek, szabályainak és klasszikus módszereinek összefoglalása". A gyakorlatban e tartalom megnevezésére is gyakran használják a rendszertan kifejezést. [3, 245. o.] A besorolástan alapvető fogalma a rendszertani egység (taxon), amely rendszertani hierarchiában bármely kategóriát jelölhet, azok összefoglaló megnevezésére szolgál. A fenti két fogalomhoz kapcsolódik még a nevezéktan (nomenklatúra) is, amely a rendszertannak az egyes rendszertani egységek megnevezésével, annak egységes szabályaival foglalkozó részterülete. [3, 245. o.]

Tágabb értelmezés szerint a rendszertan „Vmely leíró tudománynak az a része, amely az illető tudomány sajátos rendszerező elveit tárja fel, ill. ennek alapján az ismereti anyagot rendszerbe foglalja" [4, 992. o.], vagy „az osztályozás tudománya" [5], a taxonómia pedig „a tudományos osztályozás általános elveinek tudománya, lásd rendszertan" [6], „az osztályozás gyakorlata és elmélete" [7], vagy „egy osztályozási séma, amely egy ismeretanyagot tagol részekre és meghatározza az egyes részek közötti kapcsolatokat" [8]. A bemutatott meghatározások jól szemléltetik a két fogalom átfedő, illetve eltérő értelmezéseit. Mivel napjainkban a rendszertan, taxonómia fogalmak már nem korlátozódnak az élőlények rendszerezésére, ezért az eredeti tartalom megnevezésére találkozhatunk a biológiai rendszertan és alfa taxonómia kifejezésekkel is.

A rendszertan, taxonómia és nomenklatúra kifejezések egyaránt jelenthetik (jelentik) az adott szakterületet, ismeretanyagot, valamint az alkalmazásuk eredményeként létrejött konkrét osztályozási struktúrát is. Ennek megfelelően beszélünk például a Linné-féle taxonómiáról, Clausewitz katonai taxonómiájáról, vagy az informatikai biztonság rendszertanáról. A rendszertanok, taxonómiák rendeltetése mindenekelőtt egy adott szakterület (tudományterület) objektumainak, vagy azok meghatá-

rozott körének rendszerezése, osztályozása. Az osztályozás fogalmából következően egy taxonómia lényege az objektumok egy adott körének számbavétele és besorolása valamely kategóriába (rendszertani egységbe), oly módon hogy ez megkönnyítse áttekintésüket és tükrözze, jellemezze a különböző objektumok viszonyát, kapcsolatrendszerét.

A rendszerezés, osztályozás legegyszerűbb változatát az egyszerű kategória-listák képezik, ezek azonban viszonylag kevés információt hordoznak. A taxonómiák általában az alá-fölérendeltségi, általánosabb-speciálisabb jellegű viszonyokra épülő hierarchikus struktúrák, amelyekben az egyes objektumok saját kategóriáikba történő besorolással egyben magasabb szintű kategóriákba is besorolásra kerülnek (pld. kutya → ragadozó, emlős, állat, stb.).

A konkrét rendszertanok általában azonos típusú dolgok rendszerezésére szolgálnak, de alkalmassá tehetők több különböző típusú dolog rendszerezésére is. Ez megoldható különböző taxonómiák egyesítésével oly módon, hogy a különböző típusok a legmagasabb szinten kerülnek elválasztásra, majd saját szempontjaik szerint történik további besorolásuk. Erre példának tekinthető a biológiai rendszertan, amelyben eredetileg a növények és állatok, később további élőlény-csoportok ('országok') szerepelnek.

A rendszertanokkal, taxonómiákkal szemben támasztott követelmények közé lényegi és praktikus követelmények sorolhatóak. Ezek érdemi elemzésétől és részletes indoklásától most eltekintünk, a továbbiakban szükségességüket feltételezzük. A lényegi követelmények — amelyek nélkül tulajdonképpen nem beszélhetünk rendszertanról 2013 az osztályozás alapvető jellemzőiből következnek. Első követelmény, hogy pontosan meg legyen határozva, az adott rendszertan milyen objektumok rendszerezésére szolgál. A második, hogy pontosan meg legyenek határozva a besorolási szempontok. A harmadik pedig, hogy az adott körbe tartozó objektumok mindegyike egyértelműen besorolható legyen pontosan egy rendszertani egységbe. A praktikus követelmények a rendszertan hasznosságához, használhatóságához kapcsolódnak. Ezek közé olyan tulajdonságok tartoznak, mint az objektivitás, a megismételhetőség, vagy az elfogadhatóság.

A rendszertanok, taxonómiák összetevői közé elsősorban a rendszertani egységek és ezek kapcsolatrendszere, valamint a kialakítás során meghatározott, illetve a besorolás során alkalmazandó osztályozási szempont-

ok tartoznak. A rendszertani egységek (taxonok) két nagy csoportra oszthatóak, ezek az elemi (legalsó szintű) és az összetett (magasabb szintű) egységek. Az elemi rendszertani egységek (pld. biológiai rendszertan esetében a faj [egyes esetekben az alfaj]) azok a kategóriák, amelyek valamelyikébe a rendszerezendő objektumokat be kell sorolni. Ezek páronként egymást kizáróak, együttesük pedig lefedi a rendszerezni szándékozott objektumok teljes körét. Az elemi rendszertani egységek alapvető, de tudományosan és a gyakorlatban nehezen megvalósítható, megítélhető követelménye a 'természetesség', vagyis az a tulajdonság, hogy a kategóriába tartozó objektumok egy csoportba tartozása, más objektumoktól való különbözése széles körben elfogadott és emögött 'objektív', lényeges okok állnak. A 'természetesség' egyik jellemzője, hogy a kategória megnevezésére lényegében azonosan értelmezett szak-, sőt gyakran köznyelvi kifejezések alakultak ki (pld. kutya, számítógépes vírus, stb.). Az összetett rendszertani egységek az elemi egységek 'fölött' — általában több szinten — helyezkednek el, azokat foglalják általánosabb tartalmú csoportokba. Ezek alapvető szerepe az elemi egységek közötti viszonyok, a közös tulajdonságok mennyiségének, a hasonlóság — a 'rokonság' — mértékének megjelenítése. Ugyanazon elemi egységeket általában különbözőféleképpen lehet csoportosítani, ugyanazon elemi egységekre különböző rendszertanok, taxonómiák építhetőek fel. Az egyes rendszertanok, taxonómiák alapvetően kétféle úton hozhatóak létre: felülről lefelé, mintegy elméleti úton, illetve alulról felfelé, a gyakorlatban összegyűlt információk alapján. A felülről lefelé történő építkezés esetében lépésről lépésre új osztályozási szempontokat kell meghatározni, amelyek alapján fokozatosan egyre kevesebb objektumot tartalmazó rendszertani egységek alakulnak ki, amíg már egyetlen rendszertani egység esetében sincs ok, vagy lehetőség a további osztályozásra.

Az alulról felfelé történő kialakítás során nagyszámú besorolandó objektumból kiindulva lépésről lépésre, informális, vagy formális módszerek (pld. klaszter-analízis) segítségével meg kell határozni, hogy mely objektumokat 'célszerű' egy csoportba (rendszertani egységbe) sorolni, majd az így kialakított csoportokhoz meg kell határozni olyan kritériumokat, amelyek biztosítják a besorolás teljességét és egyértelműségét. A besorolási szempontok a rendszertanok, taxonómiák lényegi összetevői közé tartoznak. Ezek hiányában egy felvázolt rendszertan csak egy elképzelés, tulajdonképpen egy gyakorlattól elszakított fogalom-rendszer, amely éppen alapvető rendeltetését, a konkrét objektumok besorolását és ennek révén

kapcsolatrendszerük megismerését nem képes betölteni. A besorolási szempontok meghatározása nem egyszerű feladat. Felülről lefelé történő kialakítás esetében a kérdés az, hogy a számos lehetséges megkülönböztető jellemző, tulajdonság közül melyikeket és milyen sorrendben válasszuk ki, hogy az így kialakuló rendszertani egységek minél 'természetesebbek' legyenek. Alulról felfelé történő kialakítás esetében pedig már maga a besorolási szempont megfogalmazása is nehézségekbe ütközhet. Ráadásul a besorolási szempontoknak a bekövetkező változásokhoz, új objektumok megjelenéséhez is igazodniuk kell, azok besorolását is biztosítaniuk kell, ami jellemzően a szempontok módosítását igényli. Az elmondottakból következően tehát a rendszertanok, többszintű taxonómiák két részre oszthatóak. Az egyiket az elemi rendszertani egységek lineáris struktúrát alkotó összessége, a másikat az erre épülő magasabb szintű rendszertani egységek a gyakorlatban ma még általában hierarchikus, de elméletileg akár hálós szerkezetű összessége képezi. Az első alkotja a tulajdonképpeni, szűkebb értelemben vett taxonómiát, ennek rendszertani egységeibe kerülnek besorolásra a konkrét objektumok. A második rész pedig inkább az elemi egységekhez kapcsolódó, elemi fogalmakra épülő fogalomrendszernek tekinthető. Egyes értelmezések ehhez a megosztáshoz kötik, erre alapozzák a taxonómia és a rendszertan fogalmak közötti megkülönböztetést. Mint látható tehát, a rendszertani egységekhez kapcsolódó, objektum-csoportokat leíró fogalmak a besorolás segítése és az objektumok közötti viszonyok megjelenítése mellett egyben egy fogalom-rendszert is meghatároznak. Ezzel kapcsolatban azonban meg kell jegyeznünk, hogy az ilyen fogalom-rendszerek leírására ma már a rendszertanoknál, taxonómiáknál sokkal alkalmasabb, több információt hordozó megoldások (pld. fogalmi hálók, ontológiák) állnak rendelkezésre. Így erőteljesen hangsúlyozni kell, hogy a rendszertanok, taxonómiák rendeltetése konkrét objektumok rendszertani egységekbe sorolása és ezzel alapvető tulajdonságaik, egymáshoz való viszonyaik megjelenítése, nem pedig az ezen objektumokhoz kapcsolódó osztályozó fogalmak rendszerének meghatározása.

Rendszertan?
Az informatikai biztonság rendszertana?

A hivatkozott publikációban szereplő informatikai biztonsági rendszertannal kapcsolatban elsőként vizsgáljuk meg azt, hogy milyen célból ke-

rült összeállításra. Mindez elsőként a bevezetésben — alapvetően az informatikai biztonság oktatásához kapcsolódóan — kerül meghatározásra. Ennek során merül fel feladatként a szakterület fogalmának, tartalmának és terjedelmének tisztázása, majd rendszerezése. A rendszerezés a publikációban a szakterület — az informatikai biztonság — tartalma pontos meghatározásának előfeltételeként szerepel, de csak általánosságban. Nem kerül kifejtésre, hogy mit értünk rendszerezés alatt és az sem kerül megindokolásra, hogy ehhez szükség van-e, pontosan miért és milyen rendszertanra, illetve hogy egy rendszertan milyen szerepet játszik, menynyiben segít a szakterület tartalmának meghatározásában.

Véleményem szerint egy rendszertan önmagában nem elegendő egy szakterület tartalmának meghatározásához, legfeljebb alapvető segítséget nyújthat ahhoz, kontrollként szolgálhat és felhasználható a szakterület ismeretanyagának részekre tagolása során. Ennek indoklásához talán elegendő példaként felhozni a legáltalánosabban ismert és alkalmazott biológiai (köztük állat- és növény-) rendszertant, ami önmagában nem nyújt alapot a biológia számos szakterülete és azok tartalma meghatározásához (pld. anatómia, etológia, immunológia, szövettan stb.).

Összességében azt gondolom, hogy meg kell különböztetnünk egy szakterület ismeretanyagának rendszerezését, ezen ismeretanyag — az előbbitől oktatási célok és pedagógiai-módszertani okok miatt eltérő — oktatási célú rendszerezését, valamint a szakterület meghatározott objektumainak rendszerezését biztosító rendszertan(oka)t. Ilyen rendszertanokból, taxonómiákból egy adott szakterület esetében a kiválasztott objektumoktól függően több is lehet, azonban egyértelműnek tűnik, hogy az ismeretanyag rendszerezéséhez a szakterület alapvető — elsődleges vizsgálati tárgyát képező — objektumainak (pld. a biológia esetében az élőlények) rendszertana nyújthat segítséget. Mindez azonban már átvezet egy másik gondolatkörhöz.

A hivatkozott publikáció célja megfogalmazásának másik, lényeges hiányossága, hogy a címben foglalt kifejezés ellenére gyakorlatilag nem kerül meghatározásra: minek a rendszertanáról van szó. Mint azt korábban már bemutattuk, egy rendszertan mindig objektumok meghatározott köréhez kapcsolódik, azok rendszerezését, mélyebb megismerését szolgálja. Ennek megfelelően csak átvitt értelemben beszélhetünk az informatikai biztonság rendszertanáról (vagy a biológiai rendszertan mintájára informatikai biztonsági rendszertanról), csak akkor használhatjuk ezt a kifejezést, amennyiben már kialakult egy közmegegyezés arról, hogy ez alatt

milyen objektumok rendszertanára gondolunk. Ehhez tulajdonképpen arra kellene választ adnunk, hogy az informatikai biztonságnak mi(k) az alapvető objektuma(i). Az informatikai biztonság alapvető objektumaira vonatkozóan több elképzeléssel találkozhatunk. Ezek szinte mindegyikében szerepel a biztonság alanya (a fenyegetések által veszélyeztetett objektum), a biztonságot fenyegető veszélyeztetések, a fenyegetések bekövetkezését lehetővé tévő sebezhetőségek és a fenyegetéseket kiváltó források [9, 4-6. o]. Egy informatikai biztonsági taxonómiával foglalkozó publikációban más megközelítésben hét objektum-típus kerül megkülönböztetésre: támadók, célkitűzések, eszközök, sebezhetőségek, tevékenységek, célpontok és eredmények (tulajdonképpen biztonság-sértések) [10, 16. o.]. Az elemzett publikációban szereplő objektumok: védendő adatok, védendő tulajdonságok, védelmi feladatok, gyenge pontok (sebezhetőségek), fenyegetések, fenyegetések okai, fenyegetések forrásai, valamint a fenyegetések céljai [1, 138. o.].

Az informatikai biztonságban érintett objektumok köre tehát külön vizsgálatot igényel és ezek közül kell kiválasztani az alapvető objektumo(ka)t, amely(ek)nek a rendszertana, taxonómiája hozzásegít az informatikai biztonság ismeretanyagának, illetve oktatási anyagának feltárásához, rendszerezéséhez. Jelen publikációban ennek a kérdésnek a megalapozott feldolgozására nem vállalkozunk, azonban részletesebb indoklás nélkül megfogalmazzuk azt az álláspontot, hogy az informatikai biztonság alapvető objektumait elsősorban a biztonságot fenyegető veszélyeztetések, másodsorban a védelmi megoldások, rendszabályok képezik.

A szakirodalomban többek között találkozhatunk fenyegetés, incidens, támadás taxonómiákkal [10, 11, 12], sebezhetőség taxonómiákkal [13, 14] és védelmi rendszabályok taxonómiával [15] (amelyek feldolgozása szintén megérdemelne egy önálló publikációt). Ehhez kapcsolódóan kell megjegyezni, hogy a hivatkozott publikációban az úgynevezett Landwehr-taxonómiára vonatkozó hivatkozás [1, 138. o.] forrása hibás. A taxonómia leírása nem az ott megjelölt publikációban, hanem jelen publikáció [11] irodalmában található.

A következőkben vizsgáljuk meg, hogy a hivatkozott publikációban szereplő javaslat [1, 148-154. o.] mennyiben felel meg a rendszertanok kritériumainak. Ennek során egyelőre elsősorban csak formai szempontokat veszünk figyelembe, abból kiindulva, hogy az osztályozás a védelmi intézkedésekre irányul (ami nem teljes egészében van így, de ezzel a kö-

vetkező pont foglalkozik részletesebben). A korábbiakban már megfogalmaztuk, hogy egy rendszertan, taxonómia alapvető összetevői: a rendszertani egységek és ezek kapcsolatrendszere, valamint a besorolási szempontok. A publikációban javasolt rendszertan ezek közül elsősorban a rendszertani egységeket tartalmazza, amelyek egy változó mélységű, kettő-négy szintű hierarchiába rendeződnek, azonban csak részben rögzíti a rendszerezési, besorolási szempontokat.

Rendszerezési szempontok gyakorlatilag csak a legfelső szintű osztályozás esetében kerülnek meghatározásra. A szerző több, elvileg lehetséges szempont közül, azokat elemezve, értékelve, gyakorlati tapasztalatokat is figyelembe véve a rendszerelemeket, vagyis a fenyegetéseknek kitett (informatikai) rendszer összetevőit választja a rendszerezés alapjául. Megfogalmazása szerint „a rendszerelemeken keresztül a rendszer biztonságához szükséges valamennyi védelmi intézkedés meghatározható”. [1, 147. o.]

A felsorolt hét rendszerelemre (pontosabban összetevő típusra) épülő osztályozás esetében elsőként vizsgáljuk meg, hogy biztosítják-e az egyértelmű és páronként egymást kizáró besorolást, valamint a teljes körű lefedettséget. Az előzőekkel kapcsolatban a publikációban foglalt leírás nem elegendően részletes, többféle értelmezést is megenged. A rendszerelemek alapján történő besorolás történhet aszerint, hogy a védelmi intézkedéssel megelőzni szándékozott fenyegetés célja szerint (ha van neki!) melyik rendszerelemre irányul, vagy aszerint, hogy a védelmi intézkedés melyik rendszerelemet érinti. A javasolt osztályozásban megítélésem szerint nem teljesül a teljes körű lefedettség követelménye, ugyanis a rendszerelemek listájából hiányoznak az adatok. Márpedig ezek éppúgy — sőt sok esetben sokkal inkább — összetevői az informatikai rendszereknek és képezhetik támadás tárgyát, mint a lista más elemei.

A javasolt rendszertan nagyobb hiányossága, hogy az első szintet követően sehol sem fogalmazza meg a további osztályozás alapját, az alkalmazott osztályozási szempontokat. Egy rendszertan kellő mélységű leírása természetesen jóval meghaladja egy publikáció kereteit, ennek ellenére valamilyen mértékben be kell(ene) mutatni az alacsonyabb szintű besorolási szempontokat is. Így a felsorolt rendszertani egységek alapján csak arra lehet rámutatni, hogy az osztályozások 'valószínűleg' pontosításra, kiegészítésre szorulnak, vagyis nincs olyan szempont, amely szerint ezek a kategóriák jönnének létre, illetve hogy egyes kategóriák nem meg-

felelő helyen szerepelnek. Ezek részletes elemzésére mennyiségi okokból jelen publikáció sem vállalkozik. Bár a hivatkozott publikáció nem tűzte ki célul a rendszertanok részét képező nevezéktani kérdések rendezését, azonban a javasolt rendszertanban szereplő megnevezések sok esetben nem felelnek meg az alapvető követelményeknek. Egy rendszertan egységei, kategóriái megnevezésének biztosítania kell a besorolásban alá tartozó objektumok egyértelmű azonosítását. A megnevezések között vannak olyanok, amelyek formailag nem megfelelőek (pld. „az alkalmazás előtt", „az internet-jog" stb.); vannak olyanok, amelyek hosszúságuk miatt nem megfelelőek (pld. 1.1.3, 3.1.2, 4.2.1, stb.); és vannak olyanok, amelyek többször is előfordulnak (pld. az alkalmazás előtt ~ 1.1 és 7.5.1, elektromágneses kompatibilitás ~ 2.7.3 és 3.2.2, redundáns struktúrák ~ 3.1.2 és 6.6, rejtjelezés ~ 5.1.1 és 6.3.1, stb.). És itt most nem is tértünk ki arra a már felvetett kérdésre, hogy milyen objektumokat rendszereztünk és ezek a megnevezések vajon tényleg alkalmasak-e ezen objektumok különböző csoportjai, kategóriái leírására.

Az általános kérdések vizsgálata során végül néhány gondolat arról, hogy mik a feltételei és esélyei egy informatikai biztonsági rendszertan kidolgozásának. Megítélésem szerint egyáltalán nem lényegtelen annak a kérdésnek a vizsgálata, hogy mi lesz, lehet egy javasolt rendszertan szerepe, gyakorlati haszna. Tapasztalataim alapján és a különböző szakterületek eredményeit is áttekintve úgy gondolom, hogy egységesen elfogadott rendszertan kialakításának nagyon kicsi az esélye és ez nem csak az informatikai biztonság sajátosságaival magyarázható, hiszen a legkorábbi és leginkább elterjedt biológiai rendszertanok esetében sincs „egységesen elfogadott" változat: már a legmagasabb szintű rendszertani egységek esetében is találkozhatunk 4, 5 és 3 'országra' történő felosztással.

A különböző rendszertanok meghatározott célokkal kerülnek kidolgozásra, ebből következően: eltérő lehet a részletezés és eltérőek lehetnek az elemi rendszertani egységek; ugyanazon elemi rendszertani egységek eltérő csoportokba egyesíthetőek. Nincs ez másként az informatikai biztonság esetében sem (akármilyen objektumait válasszuk is a besorolás tárgyainak). Meg kell tehát fogalmazni a rendszertan kidolgozásának célját és egy ennek megfelelő rendszertant kell kidolgozni. Ez a hivatkozott publikáció esetében megítélésem szerint alapvetően jól van meghatározva: a cél az informatikai biztonság oktatásának megalapozását támogató, az informatikai biztonság ismeretanyagát rendszerező rendszertan.

Az előzőekben megfogalmazottak nem jelentik azt, hogy egy ilyen rendszertannak nem lehet távlatosabb, mások számára is felhasználható eredménye. A rendszertani vizsgálatok — valamelyest ismerve a szakterület szakirodalmát — hiánypótló szerepet töltenek be, de legalábbis érdemi hozzájárulást jelenthetnek a szakterület fejlődéséhez. Ehhez azonban mindenképpen további kutatómunkára, régóta kialakult és vallott véleményem szerint több kutató munkájára van szükség, amelynek során sokkal erőteljesebben kell felhasználni az általános rendszertani alapokat.

A javasolt informatikai rendszertanról

A hivatkozott publikációban javasolt rendszertan tartalmi vizsgálata előtt — mint azt a szerző is megtette — röviden át kell tekinteni a kapcsolódó alapfogalmak, de legalábbis az informatikai biztonság értelmezését, hiszen enélkül nem lehet tárgyalni az informatikai biztonság rendszertanát sem. Ennek során részletekbe nem kívánok belemenni (a kérdéskörrel kapcsolatban egy hivatkozott publikációmban [9], igaz nem a véglegesség igényével, már kifejtettem véleményemet), csak a legfontosabbnak tartott megállapításokat szeretném rögzíteni.

A publikációban foglaltakból lényegében egyetértek az informatikai biztonság, információbiztonság viszonyára vonatkozó megállapításokkal, valamint a biztonságnak állapotként, a védelemnek pedig tevékenység(rendszer)ként történő értelmezésével. A két fogalom közül magam az informatikai biztonságot tartom elsődlegesnek és az informatikai védelmet másodlagosnak. Ez eltér a szerző által megfogalmazott állásponttól, amely szerint — leegyszerűsítve — a biztonság olyan kedvező állapot, amelyben meghatározott tulajdonságokkal rendelkező védelem valósul meg. Eszerint ugyanis a biztonság meglétét, szintjét, mértékét nem önmagában, hanem a védelem állapota, jellemzői értékelésével lehet megítélni, jellemezni.

A biztonság elsődlegességéből következően megítélésem szerint elsőként meg kell határozni annak összetevőit, a biztonság alanyának azon tulajdonságait (ezen belül létét és működőképességét), amelyeknek a megengedett mértéktől eltérő megváltozása a biztonság sérülését, megsértését jelenti. [9, 5. o.] Amennyiben a biztonság alanyának az informatikai rendszereket tekintjük, az összetevők köre – mint azt a gyakorlat igazolja – az idők során változhat, bővülhet. Ehhez kapcsolódóan nem értek egyet a szerző azon besorolásával, amely a hitelességet és letagadhatatlanságot a

sértetlenség részének tekinti, ez tartalmi elemzéssel nem támasztható alá, de ezzel részleteiben most nem foglalkozok. Nem vitatva a védelem zártságának, teljeskörűségének, folytonosságának és kockázatokkal arányosságának szükségességét, ezeket csak a védelemmel szemben támasztott követelményeknek tudom értelmezni, elfogadni. Az ezekre épülő biztonság-definíció alapján ugyanis előfordulhat, hogy a biztonság [állapota] ebben az értelemben fennáll — a védelem zárt, teljeskörű, folytonos és kockázat-arányos — azonban a biztonság egyes összetevői, akár jelentős mértékben sérülnek. A biztonság meglétét objektív módon csak a biztonság összetevői érvényesülése, érvényesülésének szintje alapján lehet, szabad meghatározni. A biztonság objektív megítélésének alapját kell képezze az egyes összetevőkre vonatkozó követelmények meghatározása, vagyis pld. annak meghatározása, hogy egy adott információ illetéktelen megismerése, megsemmisítése, elérhetetlenné tétele a biztonság milyen mértékű sérülését jelenti. A biztonság megítélése tehát megítélésem szerint nem lehetséges biztonsági igények, követelmények meghatározása nélkül. Ezek ismeretében viszont gyakorlatilag érdektelen, hogy a kialakított védelem milyen, egyedül az számít, hogy az igények, követelmények érvényesülnek-e.

A fentiek alapján az informatikai védelem tartalmának a szerző által elfogadott változata [1, 143-144. o.] helyett egy tágabb, általánosabb megfogalmazást tartok megfelelőnek, amely szerint az informatikai védelem az informatikai biztonság kialakítására és fenntartására — a biztonság összetevőinek érvényesülésére — irányuló tevékenységek és rendszabályok összessége.

A következőkben a javasolt rendszertan összetevői kerülnek nagyon röviden vizsgálatra. Ezzel kapcsolatban már korábban megfogalmazásra került, hogy a hivatkozott publikációban nincs meghatározva: a rendszertan milyen objektumok rendszerezését célozza. Egyes kijelentésekből arra lehet következtetni, hogy a cél az informatikai biztonság részterületei [1, 138. o.], vagy a védelmi intézkedések [1, 147. o.] meghatározása, rendszerezése.

A fentieket alátámasztja maga a javasolt rendszertan is, mivel a benne szereplő mintegy 150 elemi rendszertani egység elenyésző kivétellel — és megfelelően pontosított megnevezéssel — védelmi intézkedésnek, védelmi tevékenységnek, védelmi eljárásnak, vagy védelmi eszköznek, de legalábbis a biztonságot megteremtését, növelését szolgáló tevékenység-

nek tekinthető. A továbbiakban ezt elfogadva veszünk sorra — a teljesség igénye nélkül — néhány fontosnak tartott kérdést.

A szerző által megfogalmazott alapvető rendszertani döntés az volt, hogy a rendszerezés alapját az informatikai rendszerek elemei képezzék, mégpedig oly módon, hogy a védelmi intézkedéseket aszerint osztályozzuk: azok mely rendszerelemre „irányulnak". E javaslat előnye, hogy valamennyi rendszerelem és „rájuk irányuló" védelmi intézkedések módszeres számbavétele elvileg biztosítani látszik valamennyi intézkedés feltárását. Ez alapvetően így is van, de egy ponton mégis hiányos: egy adott objektum biztonsága elleni fenyegetések csökkenthetőek, elháríthatóak az objektumot fenyegető szereplőkre, jelenségekre — tehát nem a védendő rendszer elemeire — irányuló tevékenységekkel is.

A javasolt rendszertanban nem szereplő védelmi intézkedések közé tartozik mindenekelőtt a biztonságot fenyegető szereplőkre, jelenségekre vonatkozó információk megszerzése, valamint a képességeiket, lehetőségeiket csökkentő, célzottan „rájuk irányuló" ellentevékenység, amelyekkel a kritikus információs infrastruktúrák vonatkozásában egy publikációban magam is foglalkoztam [15]. Megítélésem szerint ezek a tevékenységek nem zárhatóak ki a rendszertanból, e tekintetben az bővítésre szorul.

A következő észrevétel tárgya a rendszertan hierarchikus felépítése. Mint azt a bevezető pontban is megfogalmaztuk, a taxonómiák általában érvényesülő, de nem kötelező sajátossága a hierarchikus felépítés, ami azonban nem minden rendszerezés esetében valósítható meg tisztán. Egy állat- és növényrendszertani hierarchia objektív alapját tulajdonképpen ma már az evolúció adja. Ilyen alap az informatikai biztonság védelmi tevékenységei és az ezekre épülő részterületek esetében megítélésem szerint nem áll rendelkezésre, legalábbis ilyennel a szakirodalomban még nem találkoztam.

Mindennek a következményei megjelennek a javasolt rendszertanban is, ami egyrészt a több helyen is megjelenő rendszertani egységekben, de leginkább a nem egyértelmű besorolásban mutatható ki. Számos elemi rendszertani egység (védelmi intézkedés) ugyanis más helyen is lehetne, sőt pontosan megfogalmazott besorolási szempontok esetén, más helyen (is) kellene legyen a hierarchiában (pld. okos kártyák a beléptető rendszerekben, vagy az azonosítás/hitelesítés során).

A hierarchiával összefüggő problémákra megítélésem szerint — különösen az informatikai biztonság ismeretanyagának oktatási célú felhasz-

nálása szempontjából — megfontolásra érdemes az a megoldás, amely az elemi rendszertani egységek esetében megvalósítja a kölcsönös átfedésmentesség, illetve a teljeskörűség követelményét és az összetett rendszertani egységek szintjén megengedi a (legalább) hálós struktúrát, vagyis hogy ugyanaz a rendszertani egység több magasabb szintű egységbe is besorolásra kerülhessen. Így a rendszertani feladat egy osztályozási feladatra és egy fogalmi rendszer kiépítési feladatra bontható. Az osztályozási (taxonómiai) feladat esetében a hivatkozott publikációban választott 'felülről-lefelé' jellegű megoldás helyett valószínűleg célszerűbb a 'lentről-felfelé' jellegű megoldásra építeni.

Végül két gondolat az informatikai biztonság rendszertana értelmezéséhez, kialakításához. Az első lényege abban áll, hogy az informatikai biztonság rendszertana megítélésem szerint nem korlátozódhat a védelmi intézkedések rendszertanára. A két lehetséges megoldás: több rendszertan (fenyegetések, sebezhetőségek, védelmi intézkedések/eljárások/eszközök/... stb.) kidolgozása, vagy egy egységes rendszertan kialakítása, amelynek legfelső szintje osztályozza az objektumokat az előzőekben jelzett rendszertanrészekbe. Már előzetesen érdemes azonban felvetni, hogy ez utóbbi esetben is előfordulhat, hogy ugyanazon objektum — eltérő minőségében — több kategóriába is besorolható (pld. egy adott személy, mint az informatikai rendszer eleme, mint védendő objektum, és mint szándékos fenyegetést kiváltó szereplő).

A második gondolat erősebben kötődik az informatikai biztonság ismeretanyagának oktatási célú rendszerezéséhez, ami nem feltétlenül jelent szigorú rendszertani feladatot. Ennek kialakításához megítélésem szerint rendelkezni kell egy alapmodellel, amely tartalmazza az informatikai biztonságban érintett alapvető összetevőket és kapcsolatrendszerüket. Ehhez kapcsolódó elgondolások, részeredmények a szakirodalomban megtalálhatóak [10, 14, 17, 9], feltárásuk és felhasználásuk szintén elvégzendő feladatok közé tartozik.

Az alapmodellben tehát szerepelnie kell az informatikai biztonság alapvető összetevőinek, amelyek — néhány kiegészítéssel — egy változatban alapját képezhetik a kapcsolódó ismeretanyag rendszerének. Ennek megfelelően, elsősorban a struktúra jellegét bemutatandó, egy lehetséges ismeretanyag rendszerezés épülhet a következőkre:

— az informatikai biztonság fogalmi alapjai;

— az informatikai biztonság helye, szerepe, kapcsolatrendszere;

— az informatikai biztonság összetevői [megőrzendő képességek, tulajdonságok];
— az informatikai biztonságot veszélyeztető fenyegetések;
— az informatikai biztonságot veszélyeztető szereplők, jelenségek;
— az informatikai biztonság megőrzésére irányuló tevékenységek, rendszabályok;
— az informatikai védelem eljárásai, eszközei;
— az informatikai védelem részterületei és sajátosságaik;

Mindez ebben a formában természetesen csak gondolatébresztésre elegendő, jelentős további vizsgálatot, munkát igényel. Az előzőekben megfogalmazottakból következik egy további — különösen oktatási célú felhasználás esetében jelentős szerepet játszó — feladat is: az informatikai biztonság fogalmi alapjainak, fogalomrendszerének kialakítása. Ez természetesen mindig egy adott kutatói, oktatói körhöz ("iskolához") kapcsolódó eredmény, ami nem feltétlenül, nem teljes egészében egyezik meg más szakmai körök véleményével. Azonban egy képzés érdekében ennek kidolgozása megkerülhetetlen, ellenkező esetben a különböző tantárgyak, vagy oktatók által alkalmazott fogalomrendszer nem alkot egymásra épülő, egymáshoz illeszkedő, egymást erősítő struktúrát. A fogalomrendszer kialakításának napjainkban már alapvető módszere kell legyen az ontológiai megközelítés.

Összegzés, következtetések

Jelen publikáció kitűzött célja egy megjelent publikációban foglaltakhoz kapcsolódó reflexiók, kapcsolódó gondolatok megfogalmazása, közreadása volt. Ennek keretében összegzésre kerültek a rendszertan, taxonómia alapjai, majd elemzésre a javasolt rendszertan formai jellemzői, illetve tartalmi összetevői.

A hivatkozott publikációban közreadott rendszertan jelentős munkát takar, számos jó gondolatot, eredményt tartalmaz, azonban kiegészítésre, javításra is szorul. Ezek közé tartozik elsősorban az osztályozandó objektumok körének pontos meghatározása és az osztályozási, besorolási szempontok megfogalmazása. A megfogalmazott célból kiindulva feltétlenül szükségesnek látszik a rendszertan teljessé tétele, kibővítése további részekkel, az informatikai biztonsághoz kapcsolódó más jellegű objektumok taxonómiáival is. A rendszertanon kívül célszerűnek látszik az in-

formatikai biztonság ismeretanyagának oktatási célú rendszerezése és alkalmazott fogalomrendszerének kidolgozása is. Jelen publikáció — a teljesség igénye nélkül — ezen kérdések felvetésével, egyes részeiben további irányok, feladatok megfogalmazásával kívánt hozzájárulni.

Felhasznált irodalom

[1] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. Bolyai Szemle, 2008 (XVII.)/4. (137-156 o.)

[2] Magyar Nagylexikon. Tizenötödik kötet. Pon-Sek. Magyar Nagylexikon Kiadó, Budapest, 2002.

[3] Magyar Nagylexikon. Tizenhetedik kötet. Szp-Ung. Magyar Nagylexikon Kiadó, Budapest, 2002.

[4] A magyar nyelv értelmező szótára. Ötödik kötet. Mo-S. Akadémiai Kiadó, Budapest, 1966.

[5] Merriam Webster's Online Dictionary. Systematics. Merriam-Webster, Springfield, 2009. [http://mw1.m-w.com/ dictionary/systematics 2009.06.12.]

[6] Merriam Webster's Online Dictionary. Taxonomy. – Merriam-Webster, Springfield, 2009. [http://mw1.m-w.com/dictionary/ taxonomy 2009.06.12.]

[7] Wikipedia, the free encyclopedia. Taxonomy. Wikimedia Foundations, 2009.

[8] J. Radatz (szerk.): The IEEE Standard Dictionary of Electrical and Electronics Terms. Sixth Edition. – Institute of Electrical and Electronics Engineers, New York, 1996.

[9] Munk Sándor: Információbiztonság vs. informatikai biztonság. Hadmérnök különszám. A Robothadviselés 7 tudományos szakmai konferencia anyaga.

[10] John D. Howard-Thomas A. Longstaff: A Common Language for Computer Security Incidents. Sandia Report. Sandia National Laboratories, Albuquerque-Livermore, 1998.

[11] Carl E. Landwehr-Alan R. Bull-John P. McDermott-William S. Choi: A Taxonomy of Computer Program Security Flaws, with Examples. – ACM Computing Surveys, 1994 (26.)/3. (211-254. o.)

[12] Simon Hansman-Ray Hunt: A taxonomy of network and computer attacks. – Computers&Security, 2005 (24.)/1. (31-43. o.)

[13] Matt Bishop-David Bailey: A Critical Analysis of Vulnerability Taxonomies. Technical Report CSE-96-11. – Department of Computer Science, University of California, Davis, 1996.

[14] Robert C. Seacord-Allen D. Householder: A Structured Approach to Classifying Security Vulnerabilities. – Carnegie Mellon, Software Engineering Institute, Pittsburgh, 2005.

[15] Abe Usher: Towards a taxonomy of Information Assurance (IA). [http://www.sharp-ideas.net/ia/information_assurance.htm 2009.06.12.]

[16] Munk Sándor: Kritikus információs infrastruktúrákhoz kapcsolódó sajátos katonai (védelmi szférabeli) képességeket igénylő feladatok. – Hadmérnök, 2008. (III.)/3. (130-146. o.)

[17] Donald G. Firesmith: A Taxonomy of Security-Related Requirements. International Workshop of High Assurance Systems (RHAS'05), Paris, August 29-30, 2005. [http://www.sei.cmu.edu/programs/ acquisition-support/publications/ taxonomy.pdf 2009.06.26.]