Muha Lajos CISM
főiskolai docens
Gábor Dénes Főiskola

Informatikai biztonsági szabványok és irányelvek (a nemzetközi és a hazai szabályozás helyzete)

1. Bevezető

Az egyes országokban, illetve a nemzetközi szervezetekben folyamatosan fejlesztik, bővítik az informatikai biztonságra vonatkozó szabványokat, irányelveket. Sajnos, sok esetben még az ezzel foglalkozó szakemberek sem tudnak eligazodni ezek között, pedig nagyon fontos, hogy minden szabványt csak arra használjunk, amire készült. Más az informatikai, más a biztonsági és más az informatikai biztonsági szabványok felhasználhatósága. Mások az informatikai biztonság technológiai kérdéseit szabályozó és megint mások az informatikai biztonságirányítási rendszer megvalósítására és ellenőrzésére szolgáló iránymutatások. Ebben a kérdésben kíván az előadás iránymutatással, segítséggel szolgálni.

Az előadásban alábbi szabványok és ajánlások felhasználási területei kerülnek elemzésre és összehasonlításra:

- ITIL (IT Infrastructure Library)
- COBIT (Control Objectives for Information and Related Technology)
- ISO/IEC 15408 (Common Criteria)
- ISO/IEC 17799:2005 (BS-7799-1)
- ISO/IEC TR 13335
- ISO/IEC 27001:2005 (BS-7799-2)
- NIST SP 800 sorozat
- NATO C-M(2002)49
- MeH ITB 8. számú ajánlása
- MeH ITB 12. sz. ajánlása
- MIBÉTS
- MIBIK

2. ITIL

Az ITIL kezdetben brit szabvány (BS 15000) és kormányzati ajánlás volt, a közigazgatási területen általában megkövetelték az alkalmazását. Mivel a gyakorlati alkalmazás tapasztalatai kedvezőek voltak, a módszertant a piaci környezetben is egyre inkább használni kezdték. Az ITIL-t egyre inkább használni kezdték a szigetországon kívül is. Egyre több országban alakultak helyi Fórumok, ezek összefogására létrejött az IT Service Management Forum International, amely a nemzeti fórumokon keresztül egyrészt segítette az ITIL terjedését, másrészt ügyelt arra, hogy az egységes maradjon. Az ITIL mára „de facto" nemzetközi szabvánnyá vált, amelynek több országban működik felhasználói szervezete, meghatározó módszertanná vált az informatikai infrastruktúra és informatikaszolgáltatás irányítása területén. Az ITIL-t számos nemzetközi informatikai cég is elfogadta és támogatja, így például a Hewlett Packard, Microsoft, IBM stb. Ezek a cégek saját gyakorlatukba beépítették az ITIL terminológiáját és megközelítését. Sok szolgáltató, amely támogató szoftver eszközöket kínál, igyekszik azokat ITIL konformmá tenni, hogy ezzel is javítsa piaci pozícióját.

A MeH ITB Infrastruktúra menedzsment címen 15. számú ajánlásaként kiadta. A 3.1 verziót a Széchenyi-terv támogatásával 2002. novemberében honosították.

A MeH ITB Infrastruktúra menedzsment címen 15. számú ajánlásaként kiadta. Az ITIL 3.1 verzióját a Széchenyi-terv támogatásával 2002. novemberében honosították.

Az ITIL, *„Az informatikaszolgáltatás módszertana"* egy az informatika, mint szolgáltatás egészére kiterjedő, nemzetközileg széles körben elfogadott dokumentum. Az ITIL Biztonságirányítás (Security Management) kötete a BS7799 szabványt használja hivatkozásként, amikor a létező ITIL folyamatokat bővíti a biztonságirányítással.

3. COBIT

A *Control Objectives for Information and Related Technology* (COBIT) támogatói, az Information Systems Audit and Control Foundation (Információs Rendszerek Ellenőrzésével és Vizsgálatával foglalkozó Alapítvány) és az IT Governance Institute elsősorban azzal a céllal dolgozták ki az *Összefoglaló áttekintés,* a *Keretrendszer,* az *Ellenőrzési irányelvek,* a *Vezetői útmutató,* az *Auditálási útmutató* és az *Alkalmazási módszerek* elnevezésű kiadványokat (együttesen a Termék.), hogy forrásanyagot biztosítnak az ellenőrzési

szakemberek számára. A COBIT üzleti folyamatokra helyezi a fő hangsúlyt, és az ezeket támogató informatikai folyamatokhoz kapcsolódóan, amelyek négy területre összpontosít: tervezés és szervezet; beszerzés és üzembe állítás; informatikai szolgáltatás és támogatás valamint felügyelet. A COBIT az informatikai rendszerek szervezéséhez, és különösen az ellenőrzéséhez szükséges irányelveket tartalmazó dokumentum, amely a biztonság kérdésére nagy hangsúlyt fektet, de annak részleteivel nem foglalkozik.

Az ISACA és az IT Governance Institute 2004-ben a *Mapping of ISO/IEC 17799:2000 with COBIT* (2004) kiadványban már az ISO/IEC 17799 szabvánnyal hangolja össze a COBIT Framework-ben leírt informatikairányítási keretrendszert. A 2005-ben kiadott *Information Security Harmonization* az informatikai biztonsággal foglalkozó szabványok és ajánlások kissé sajátos szemléletű összehasonlítása.

4. ISO/IEC 15408 (Common Criteria)

A TCSEC és az ITSEC problémáinak feloldására, az Európai Közösség, valamint az amerikai és a kanadai kormányok támogatásával kidolgozásra került Common Criteria (CC) dokumentum, azaz az ISO/IEC 15408 (*Common Criteria for Information Technology Security Evaluation*, *version 2.0*) szabvány elsősorban technikai jellegű, főleg az informatikai termékek gyártóinak ad támogatást. Nagyon részletes és megbízható követelményeket, eljárásokat biztosít az informatikai eszközök biztonsági minősítésére. Nem tartalmaz ugyanakkor követelményeket az informatikai rendszerek üzemeltetésével, működtetésével kapcsolatban a felhasználó szervezetek számára.

5. BS 7799 (ISO/IEC 27000, ISO/IEC 17799)

A Brit Szabványügyi Hivatal *„BS 7799 Part 1, Code of practice for information security management”* kiadványa. Ez utóbbit 2000. augusztusában ISO/IEC 17799:2000 számon „***Information Technology – Code of practice for information security management***” néven nemzetközi szabványként fogadták el. Az eddig többségében termékorientált szemlélet egy szervezeti szintű informatikai biztonságmenedzsment központú szemlélet váltotta fel. Az ISO/IEC 17799 szabvány alapvetően abban különbözik a korábbi informatikai biztonsági ajánlásoktól, hogy nem követelményeket ír elő, hanem – a **minőségbiztosítás**ról szóló ISO 9000 szabványhoz hasonlóan – *a teljes körű informatikai biztonság* megteremtéséhez

szükséges szervezési, szabályozási szempontrendszert adja meg. A szabvány felhasználóinak a biztonsági követelményeket, intézkedéseket a szervezet üzleti céljaiból és stratégiájából kell levezetniük. Ez a szabvány már alkalmas arra, hogy a megfelelő akkreditálás és tanúsítási eljárások alkalmazásával lehetővé váljon a teljes informatikai rendszer értékelése és tanúsítása.

Ellentmondásosnak tűnhet, hogy a BS 7799 csak a figyelembe veendő biztonsági követelményeket és a megvalósítandó védelmi intézkedéseket írja le, de nem foglalkozik a megfelelőségi és ellenőrzési követelményekkel. Ezt a BS 7799 2. része tartalmazza.

A BS 7799 első része 2000-ben ISO/IEC 17799 számon, majd a 2. rész 2005-ben ISO/IEC 27001 számon nemzetközi szabvány lett.

6. ISO/IEC 17799:2005

Az ISO/IEC 17799 szabvány nem csak azért kiemelt fontosságú, mert a teljes szervezetre vonatkozó, az összes rendszerelem csoportot átölelő informatikai biztonsági követelményeket és védelmi intézkedéseket tartalmazza, de a különböző nemzeti dokumentumok közül ez vált nemzetközi szabvánnyá, és emellett a „de facto" nemzetközi szabvánnyá vált ITIL is ezt használja hivatkozási alapként.

Az ISO/IEC 17799 szabványt – bár kritikák is érik – a világ, és különösen az Európai Unió mind több országában fogadják el a különböző szervezetek informatikai rendszerük biztonságának alapjaként.

2005. június 10-én kiadták ISO/IEC 17799:2005 számon az informatikai biztonság e szabványának új verzióját.

A szabvány új címe: Informatika– Biztonsági technikák – Kézikönyv az informatikai biztonság irányításához[1]. A szabvány fő fejezetei megegyeznek a 2000. évi kiadásban szereplőkkel, de kiegészült egy új informatikai biztonsági eseménykezelési (incidensmenedzsment) fejezettel. Változott viszont az egyes pontokhoz írt útmutatók struktúrája, új elemek is belekerültek (pl. olyanok is, melyek a BS 7799-2:2002 fő részében szerepelnek).

A Magyar Szabványügyi Testület 2002. évben magyar szabványként kiadta „Az informatikai biztonság menedzsmentjének eljárásrendje" címen az ISO/IEC 17799:2000

[1] Information technology – Security techniques – Code of practice for information security management

szabványt. Sajnos az MSZ ISO/IEC 177999:2002 magyar szabványnak van egy nagy hibája. Nem az informatikai és a biztonsági szaknyelvezetet ismerő fordító kezéből került ki, ezért számos, a szakmában értelmezhetetlen kifejezést tartalmaz (pl.: user=használó, vagy terminal time-out=végállomás időlekapcsolás), ami miatt a magyar felhasználók nem szívesen használják. Az ISO/IEC 17799:2005 szabvány magyar nyelvű kiadására várhatóan 2006-ban kerül sor.

7. ISO/IEC 27001

A BS 7799 2. részének fejlesztése során került előtérbe a szervezeti szintű informatikai biztonság irányítási rendszer (ISMS[2]), amely alapvetően meghatározza a 2. rész szellemét. Ettől a 2. rész még az első résznél is nagyobb jelentőségű lett, mert meghatározza a megfelelőségi és ellenőrzési követelményeket, azaz a szervezetek vezetése számára meghatározza azokat a teendőket, amelyekkel az informatikai biztonsági rendszert irányíthatja, csökkentheti a maradék kockázatokat, valamint ellenőrizheti a jogszabályoknak, a tulajdonosok és az ügyfelek által támasztott biztonsági követelményeknek való megfelelést.

A BS 7799 második részét 2002-ben módosították az ISO 9001:2000 és az ISO 14001:1996 szabványokkal való harmonizáció miatt. Az aktuális változat a BS 7799 Part 2:2002, Information security management systems – Specification with guidance for use. Ez utóbbit fogadta el a Nemzetközi Szabványügyi Testület **ISO/IEC 27001:2005** (*Informatika – Biztonsági technikák – Informatikai biztonság irányítási rendszere – Követelmények*.) számon nemzetközi szabványként.

2005. október 14-én a Nemzetközi Szabványügyi Testület kiadta az **ISO/IEC 27001:2005** szabványt, *Informatika – Biztonsági technikák – Informatikai biztonság irányítási rendszere – Követelmények*[3]. A szabvány a BS 7799-2:2002 brit szabvány nemzetközi megfelelője.

Az új szabvány megjelenése az informatikai biztonság irányítási rendszerének fejlesztésére és nemzetközi szabványként történő népszerűsítésére fordított munka eredménye.

Az új számozás nem következik a régiekből, hanem egy új biztonsági szabványcsalád, az ISO 27000 megteremtésének tervéből fakad. (Lehet, hogy a számozás összefüggésben van azzal, hogy a Nemzetközi Szabványügyi Testület informatikai bizottságának a biztonsággal

[2] ISMS = Information Security Management System
[3] Information technology – Security techniques – Information security management systems – Requirements

foglalkozó albizottsága a 27-es számú[4]!?). Az ilyen tevékenység célja valamennyi, az informatikai biztonság irányításával (menedzselésével) foglalkozó szabvány egyetlen sorozatba gyűjtése. A szabványcsalád jelenleg tervezett tagjai:

- **ISO 27000** – szószedet és terminológia (definíciók a sorozat összes szabványához).
- **ISO 27001** – az informatikai biztonság irányítási rendszere (BS 7799-2:2002), a szervezet auditálásához szükséges (megfelelőségi) előírások. Az ISO/IEC 27001 szabványt 2005. 10. 14 –én közzétették ISO/IEC 27001:2005 számon.
- **ISO 27002** – a jelenlegi ISO/IEC 17799:2005 szabvány utódja. Az informatikai biztonság irányítása gyakorlati előírásait, ellenőrzési célokat és a legjobb gyakorlatot (best practice) írja le.
- **ISO 27003** – Az ISO/IEC 27000 szabvány implementálásához szükséges tanácsokat és útmutatókat fogja tartalmazni.
- **ISO 27004** – egy új szabvány lesz, amely az informatikai biztonság mérésével fog foglalkozni, abból a célból, hogy az informatikai biztonság irányítási rendszerének hatékonyságát mérni tudjuk. Jelenleg előkészületben van az ISO/IEC 27004 szabvány, amely az *Informatika – Informatikai biztonság irányítása*[5] előzetes címen fut.
- **ISO 27005** – a BS 7799-3 tervezett új része, amelyik az informatikai biztonság kockázatkezelésével foglalkozik.

8. ISO/IEC TR 13335

Az informatikai biztonság területén egyre többen használják az *ISO/IEC TR 13335 – Guidelines for the Management of IT Security*[6] (GMITS) műszaki beszámolót. Az ISO/IEC TR 13335 nem szabvány, annak ellenére, hogy a Nemzetközi Szabványosítási Szervezet és a Nemzetközi Elektrotechnikai Bizottság szabványsorozatának részeként került kiadásra, de „Technical Report”-ként. Ebben az esetben ez a megoldási lehetőségek leírását jelenti, és ezt csak akkor vizsgálják felül, ha az abban foglaltak már nem érvényesek, vagy már nincsenek használatban.

[4] A JTC 1 bizottság SC 27 albizottsága az informatikai biztonsági technikák (IT Security techniques) területén történő szabványosítást végzi
[5] Information technology – Information security management
[6] Segédlet az informatikai biztonság irányításához

Az ISO/IEC TR 13335 öt részből áll:

1. Az informatikai biztonság koncepciója és modellje (Concepts and models for IT Security),
2. Az informatikai biztonság irányítása és tervezése (Managing and planning IT Security),
3. Az informatikai biztonság irányításának megoldásai (Techniques for the Management of IT Security),
4. A védelmi eljárások kiválasztása (Selection of Safeguards),
5. Hálózatbiztonsági megoldások (Safeguards for External Connections).

A Magyar Szabványügyi Testületnél jelenleg előkészítés alatt áll az ISO/IEC TR 13335 első és második részének magyar kiadása.

9. MeH ITB ajánlások

A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) „Informatikai biztonsági módszertani kézikönyv" címet viselő, 1994-ben kiadott MeH ITB 8. számú ajánlása a brit kormány Központi Számítógép és Távközlési Ügynökség (Central Computer and Telecommunications Agency) „CCTA Risk Analysis and Management Method" és az északrajna-vesztfáliai kormány „Informationtechnik Sicherheitshandbuch" felhasználásával, valamint az EU informatikai ajánlásai és a hazai jogszabályok alapján készült. A kézikönyv célja a szervezetet az informatikai biztonsági koncepciójának kialakítására történő felkészítés volt. A biztonsággal kapcsolatos legfontosabb tudnivalók, valamint az informatikai biztonság és a szervezet összbiztonsága közötti összefüggések meghatározó elemei a kézikönyvhöz csatolt mellékletekben találhatók meg. *A MeH ITB 8. számú ajánlását, mint az informatikai biztonság – CRAMM alapú – kockázatelemzési módszertanát a közigazgatás területén kívül is elterjedten használják.*

A MeH ITB kezdeményezésére 1995-ben kezdődött meg a következő hazai ajánlás kidolgozása, amelyet 1996. decemberére véglegesítettek, és az *Informatikai Rendszerek Biztonsági Követelményei* címmel, mint a *MeH ITB 12. sz. ajánlás* vált de facto szabvánnyá. Az *Informatikai Rendszerek Biztonsági Követelményei kidolgozásánál elsődleges szempont volt, hogy ne csak a logikai védelem előírásait tartalmazza, hanem jelenjenek meg benne az adminisztratív és a fizikai védelem követelményei is.* A logikai védelem (hardver, szoftver, hálózatok) esetében az ITSEC lett adaptálva, ugyanakkor részletes követelményeket és védelmi intézkedéseket tartalmaz az informatikai biztonság adminisztratív és a fizikai védelem területeire, a szervezeti, személyi és fizikai biztonság kérdéseire is. A gazdasági élet

számos szereplője a saját biztonsági politikája kialakításakor figyelembe vette a 12. sz. ajánlást, több esetben a mai napig is belső szabályzóként, követelményrendszerként használják a biztonsági követelmények meghatározására. Mivel ma már az ITSEC dokumentumot nem használják, így a 12. számú ajánlás is elavulttá vált.

10. Magyar Informatikai Biztonsági és Tanúsítási Séma (MIBÉTS)

Az CC feldolgozására és honosítására irányuló munka hazánkban 1997-ben kezdődött, majd 1998-ban a MeH ITB 16. sz. ajánlásaként *„Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana”* címen, mint a Common Criteria 1.0 változatának hazai feldolgozása kiadásra került. A Magyar Szabványügyi Testület 2002. évben magyar szabványként kiadta „Az informatikai biztonságértékelés közös szempontjai” címen az ISO/IEC 15408 szabványt

A Magyar Információs Társadalom Stratégia készítéséről rendelkező 1214/2002. (XII.28.) sz. Kormányhatározat többek között az alábbi feladatot tűzi ki: „4.2. Ki kell alakítani az informatikai alkalmazások minőségének és biztonságának hiteles tanúsítási rendjét, az ehhez szükséges jogszabályok megalkotásával és intézményrendszer felállításával.”

A kormányhatározat végrehajtásával párhuzamosan hazánk csatlakozott a Common Criteria (CC, Közös szempontrendszer, MSZ ISO/IEC 15408) egyezményhez. Csatlakozásunkkal kapcsolatosan elkezdődött egy saját nemzeti séma, a Magyar Informatikai Biztonsági Vizsgálati és Tanúsítási Séma (MIBÉTS) felállítását, melynek során ki kell alakítani a megfelelő bevizsgálási, auditálási folyamatokat az informatikai eszközök biztonságának ellenőrzésére.

Részben CC egyezményhez való teljes csatlakozás támogatására, a hazai hiteles tanúsítási rendszer kialakítását elősegítendő, részben a nem nemzetközi alkalmazásra szánt informatikai termékek biztonsági bevizsgálását elősegítendő készült el a Common Critéria-n alapuló, a Common Evaluation Methodology for Information Technology for Information Technology Security egyszerűsített (honosított) változataként a MIBÉTS.

A MIBÉTS az új informatikai rendszerek bevezetése, a működő rendszerek – az informatikai sajátosságokból adódó - folyamatos megújítása, fejlesztése során, a tervezéstől a bevezetésig figyelembe veendő a technológiai biztonsági szempontokat kialakításához és értékeléséhez

nyújt támogatást. A MIBÉTS dokumentumok az informatikai rendszer kialakításáért felelős vezetők, szakemberek (informatikai termékfejlesztők, rendszer-integrátorok), továbbá a technológia szempontú értékelést és tanúsítást végzőknek szól.

A MIBÉTS dokumentumok az Információs Társadalom Koordinációs Tárcaközi Bizottság (ITKTB) honlapján, az Informatikai Biztonság Albizottság (INBA) dokumentumai között érhető el a http://www.itktb.hu/engine.aspx?page=dokumentumtar&docstorefolder=200 címen.

11. Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK)

Újra utalva a Magyar Információs Társadalom Stratégia készítéséről rendelkező 1214/2002. (XII.28.) sz. Kormányhatározat 4.2. pontjára, az Informatikai és Hírközlési Minisztérium 2004-ben úgy döntött, hogy a nemzetközi trendekkel összhangban kidolgoztatja a szervezeti szintű informatikai biztonság követelményeit és a vizsgálat rendjét – mint Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlásait – az **ISO/IEC 17799 nemzetközi szabvány** alapján, az **ISO/IEC TR 13335 szabvány**, továbbá a **NATO (*Security within the North Atlantic Treaty Organisation* (NATO) – C-M(2002)49)** és az **Európai Unió (*Európai Unió Tanácsának Biztonsági Szabályzata* (2001/264/EK)** releváns szabályozásai figyelembe vételével.

A szervezeti szintű informatikai biztonsági ajánlástervezetek közös, összefoglaló elnevezése a Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK). A MIBIK – jelenleg – két kötetből áll. Az első *Az Informatikai Biztonság Irányításának Követelményrendszere (IBIK),* a második *Az Informatikai Biztonság Irányításának Vizsgálata (Tanúsítása) – módszertan (IBIV)* címet viseli.

Az IBIK azoknak ad segítséget az informatikai biztonság szervezeti szintű kezeléséhez, akik saját szervezetükben a biztonság kezdeményezéséért, megvalósításáért és megtartásáért felelnek. A követelményrendszer átfogó tájékoztatást ad a szervezetek vezetésének és szakembereinek az informatikai biztonsággal kapcsolatos követelményekről. Az IBIK célja a szervezetek részére egységes elveken nyugvó, a nemzetközi szabványokhoz és ajánlásokhoz igazodó olyan hazai előírások biztosítása az informatikai biztonságának megteremtéséhez. Az IBIK szerkezetében pontosan követi az ISO/IEC 1779:2000 nemzetközi

szabványét, és tartalmában is többnyire erre épül, a már fent említett további anyagok felhasználásával.

Az IBIK alapján elkészíthetők az informatikai biztonság alapdokumentumai (az informatikai biztonságpolitika, az informatikai biztonsági stratégia és az Informatikai Biztonsági Szabályzat), segítséget ad a biztonságos működéshez szükséges szervezeti struktúra, a személyi, a fizikai és az elektronikus információvédelem kialakításához.

Az **IBIV** célja a közigazgatási és a gazdasági kormányzati szféra informatikai rendszereinek biztonsági vizsgálatához módszertan biztosítása, és tanúsítására vonatkozó igényeinek eredményes kielégítése, amely során a szervezet vezetése bizonyosságot szerezhet arról, hogy a szervezet informatikai rendszere kielégíti saját biztonsági céljait, illetve az érdekelt külső felek meggyőződhetnek arról, hogy az őket is érintő biztonsági fenyegetéseket kellően figyelembe veszik a tanúsított szervezet informatikai rendszerében hozott ellenintézkedésekkel.

A szervezetek vezetése és belső ellenőrző szervei által végrehajtott ellenőrzések mellett a nemzetközi, de már a hazai gyakorlatban is egyre jobban terjed – megfelelő felkészülés után – a BS 7799 (ISO/IEC 17799) szabványnak való megfelelést bizonyító audit elvégzése.

A vizsgálati módszertan alapját a MeH ITB 8. számú ajánlás, a BS 7799-2:2002 szabvány, és az ehhez kapcsolódó PD 3001 – PD 3005 munkadokumentumok képzik.

A MIBIK az Információs Társadalom Koordinációs Tárcaközi Bizottság (ITKTB) honlapján, az Informatikai Biztonság Albizottság (INBA) dokumentumai között érhető el a http://www.itktb.hu/engine.aspx?page=dokumentumtar&docstorefolder=200 lapon, „*Az informatikai biztonság irányításának vizsgálata*” címen.