INFORMATIKAI BIZTONSÁG ALAPJAI

1. előadás

Göcs László
főiskolai tanársegéd
Neumann János Egyetem GAMF Műszaki és Informatikai Kar
Informatika Tanszék

2018-19. 1. félév

Elérhetőség, információ

- Göcs László
- Informatika Tanszék 1. emelet **116**-os iroda
- **gocs.laszlo@gamf.uni-neumann.hu**

www.gocslaszlo.hu/oktatas

Félévi követelmény

- **2 db** zárthelyi dolgozat megírása a **6.** és a **12.** héten. A dolgozatok 40 percesek, mindegyikén **50 pont** érhető el.

- Ha a 2 dolgozat össz. pontszáma nem éri el az **50 pontot**, akkor a **13. héten a teljes féléves anyagból Pót Zh**-t kell írni, ami 80 perces.

- A vizsgára bocsátás feltétele - aláírás:

  a zárthelyi dolgozatok sikeres megírása (50% - 50 pont).

VIZSGA (írásbeli + szóbeli - 11 tétel)

A félév tematikája

- Az **informatikai biztonság fogalma**, tartalma. ITB12, IBSZ, **károk** jellege, fajtái, kár érték szintek.
- Biztonsági osztályok (A,F,K), megbízható működés, **rendelkezésre állás**.
- IT biztonsági technikák: a **felhasználók azonosításának** eszközei,(vonalkód, tudásalapú, birtokalapú és biometria). **Jelszavak fontossága**, jelszó választás problémái, jelszófeltörések megakadályozása.
- **Vállalati biztonság**. Kliens és Szerver oldali biztonság, központosított menedzsment, adatvédelem, szerverszobák kialakításának szempontjai. IDS rendszerek.
- **Titkosítás, hitelesítés**. Kriptográfia, szteganográfia. Történeti áttekintés (de Vigenére, Enigma).

A félév tematikája

- Szimmetrikus kulcsú titkosítás. Aszimmetrikus kulcsú titkosítás. **Titkosítási módszerek** operációs rendszerekben.
- **Emberi tényező az IT biztonságban**. Social Engineering. Helyi gépek biztonsága, PC védelmi lehetőségek. Adatmegsemmisítés lehetőségei.
- **Tűzfalak** fajtái és lehetőségei. A Proxy szerver. **Routerek** hozzáférési listái.
- Vírusok, Hackerek.
- **Törvények** az informatikában.
- Az **ITIL** szerepe és ismertetése.

Az informatikai biztonság fogalma

A központban áll egy **érték**, az adatok által hordozott **információ**, amelyet az egyik oldalról **támadnak**,

a másik oldalon az információk tulajdonosa pedig **védi** azt.

Mindkét fél egymástól **független**, egymás számára ismeretlen stratégiával igyekszik megvalósítani támadási, illetve védelmi szándékait.

A **védő** mindig többet **veszít**, mint amit a támadó nyer.

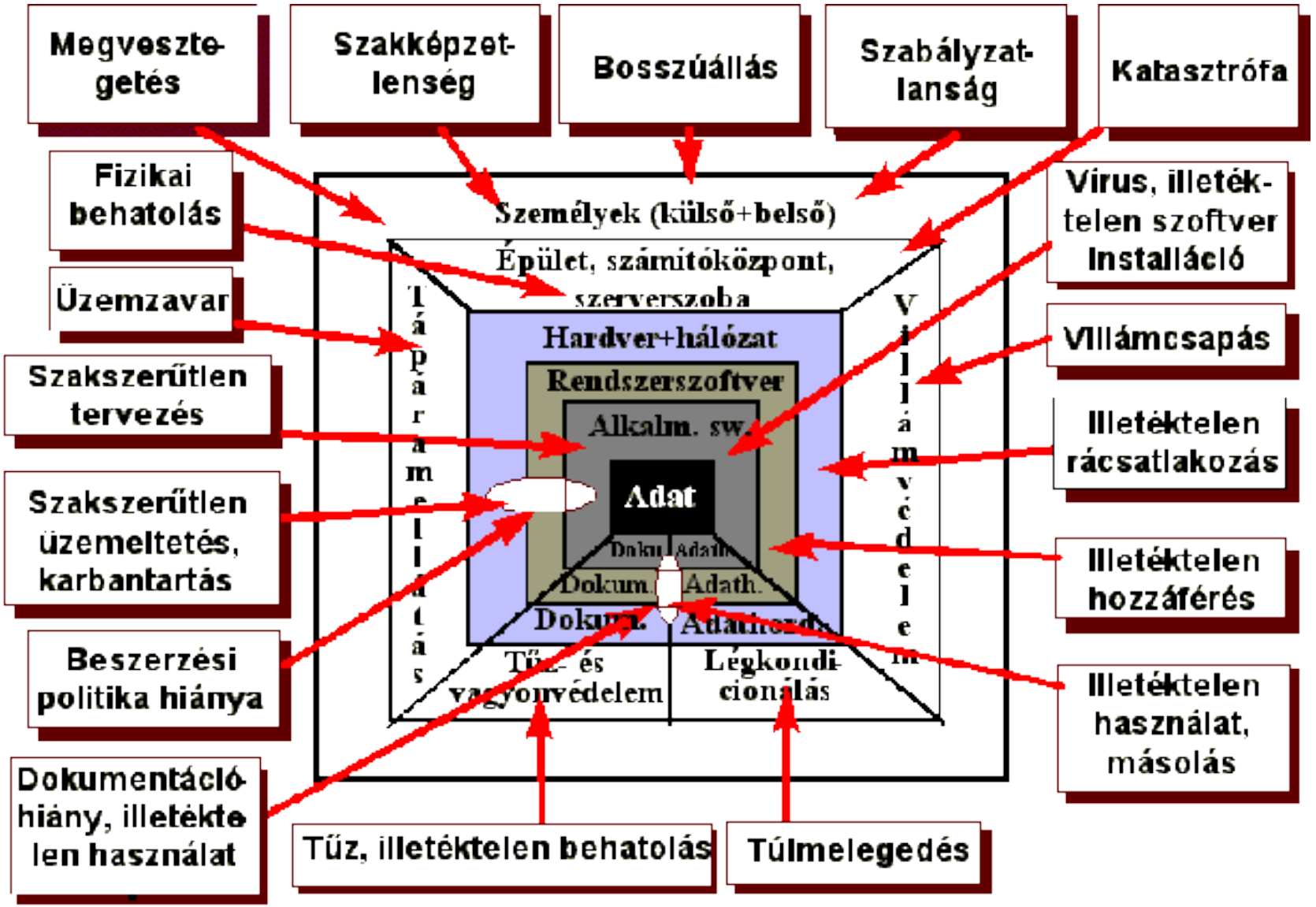
A kár nem csak anyagi lehet, hanem

- Politikai
- Erkölcsi
- Üzleti stb.

Az adatot, mint a **támadások alapvető célját** a következő rendszerelemek veszik körül:

- az informatikai rendszer fizikai környezete és infrastruktúrája,
- hardver rendszer,
- szoftver rendszer,
- kommunikációs, hálózati rendszerek,
- adathordozók,
- dokumentumok és dokumentáció,
- személyi környezet (külső és belső).

MINDEGYIKRE KÜLÖNBÖZŐ FENYEGETETTSÉGEK HATNAK!

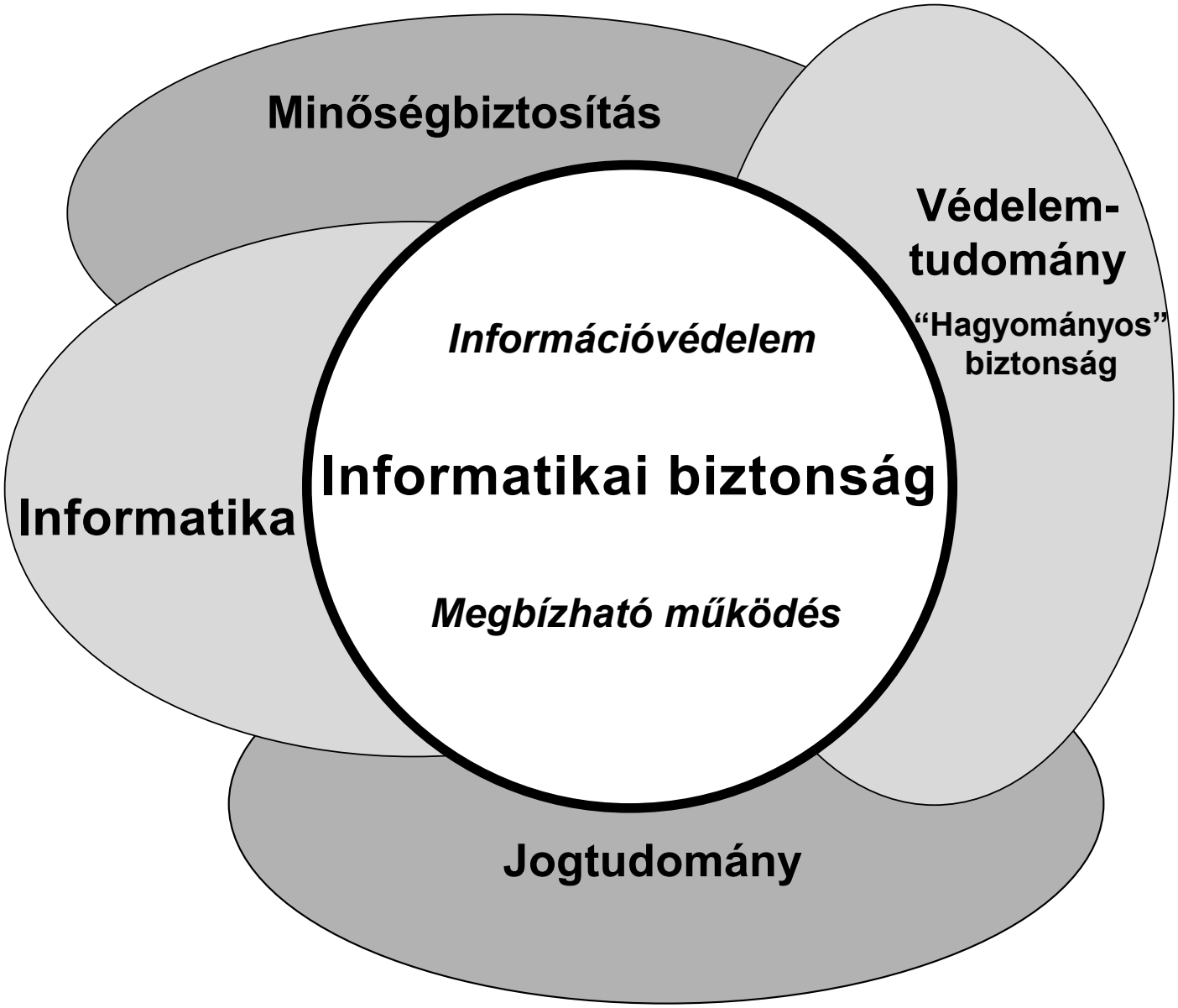

Megveszte-getés
Szakképzet-lenség
Bosszúállás
Szabályzat-lanság
Katasztrófa
Fizikai behatolás
Üzemzavar
Szakszerűtlen tervezés
Szakszerűtlen üzemeltetés, karbantartás
Beszerzési politika hiánya
Dokumentáció-hiány, illetékte-len használat
Személyek (külső+belső)
Épület, számítóközpont, szerverszoba
Hardver+hálózat
Rendszerszoftver
Alkalm. sw.
Adat
Dokum.
Adath.
Tűz- és vagyonvédelem
Légkondi-cionálás
Tűz, illetéktelen behatolás
Túlmelegedés
Vírus, illeték-telen szoftver Installácló
Villámcsapás
Illetéktelen rácsatlakozás
Illetéktelen hozzáférés
Illetéktelen használat, másolás

Az **informatikai biztonságot** úgy határozhatjuk meg, hogy az az állapot amikor az informatikai rendszer védelme - a rendszer által kezelt adatok

- bizalmassága,
- hitelessége,
- sértetlensége és
- rendelkezésre állása, illetve a
- rendszerelemek rendelkezésre állása és
- funkcionalitása szempontjából

- **zárt, teljes körű, folyamatos és a kockázatokkal arányos**.

- **Teljes körű védelem** alatt azt értjük, hogy a védelmi intézkedések *a rendszer összes elemére* kiterjednek.
- **Zárt védelemről** *az összes releváns fenyegetést figyelembe vevő védelem* esetén beszélünk.
- A **folyamatos *védelem*** *az időben változó körülmények és viszonyok ellenére is megszakítás nélkül* megvalósul.
- A **kockázattal arányos védelem** esetén egy kellően nagy időintervallumban *a védelem költségei arányosak a potenciális kárértékkel.*
- A védelem akkor **kielégítő erősségű** (mértékű), ha a védelemre akkora összeget és olyan módon fordítanak, hogy ezzel egyidejűleg a releváns fenyegetésekből eredő kockázat (kárérték × bekövetkezési gyakoriság) a szervezet számára még elviselhető szintű vagy annál kisebb.


Minőségbiztosítás
Védelem-
tudomány
“Hagyományos”
biztonság
Információvédelem
Informatikai biztonság
Informatika
Megbízható működés
Jogtudomány

Az informatikai biztonság két alapterületet foglal magába:

- **információvédelem**, amely az adatok által hordozott információk sértetlenségének, hitelességének és bizalmasságának elvesztését hivatott megakadályozni.

- az **informatikai rendszer megbízható működése** területét, amely az adatok rendelkezésre állását és a hozzájuk kapcsolódó alkalmazói rendszerek funkcionalitását hivatott biztosítani.

Számítógép biztonság

- Helyi autentikáció (belépési azonosítás, BIOS…)
- Jelszavak fontossága (xX12!3@A5g4%)
- Hardvervédelem (adatmegsemmisítés, adatvisszahozás)

Hálózati biztonság

- Vezetékes hálózati rendszerek (DHCP-MAC)
- Központi menedzselés (AD, Group Policy…)
- Vezeték nélküli hálózatok (WPA2/PSK…)
- Hálózat megosztási jogosultságok (nyomtató, mappa…)

Személyi biztonság

- Beléptető rendszerek (Smart kártya)
- Biometria (ujjlenyomat, retina…)
- Alkalmazottak (Social Engineering)

Adatok biztonsága

- RSA titkosítás
- Digitális aláírás
- Email biztonság

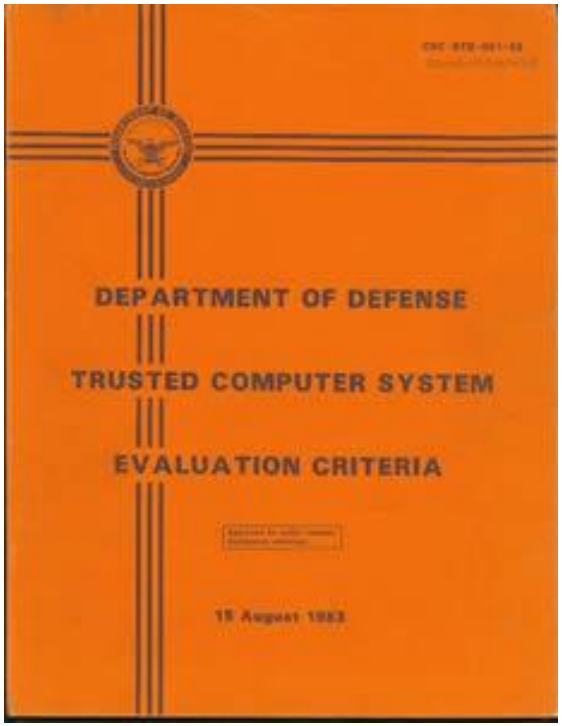
Szerver biztonság

- RAID technológia
- Backup
- Tükrözés

TCSEC

- **TCSEC** (**T**rusted **C**omputer **S**ystem **E**valuation **C**riteria = Biztonságos Számítógépes Rendszerek Értékelési Kritériumai = orange book)

Az USA informatikai biztonsággal kapcsolatos követelményrendszere, kormányzati és katonai rendszerek alkalmazásában kötelező.



ITSEC

- **ITSEC** (**I**nformation **T**echnology **S**ecurity **E**valuation **C**riteria = Információtechnológia Biztonsági Értékelési Kritériumai)

Az EU országaiban ezt a követelményrendszert fogadják el és használják a **felhasználók és a piaci szektorok**.

ITSEC 10 funkcionalitási osztálya:

- **F-C1:** korlátozott hozzáférés-védelem
- **F-C2:** korlátozott és ellenőrzött hozzáférés-védelem, a hozzáférési jogokat csoportoknak vagy egyes személyeknek határozzák meg.
- **F-B1:** címkézett kötelező hozzáférés-védelem.
- **F-B2:** strukturált hozzáférés-védelem.
- **F-B3:** elkülönített védelmi területek.
- **F-IN:** nagy integritású rendszerek osztálya (azonosítás, hitelesítés, jogkezelés)
- **F-AV:** magas rendelkezésre állást igénylő rendszerek osztálya.
- **F-DI:** adatmozgatásnál magas adatintegritást bizt. Rendszerek. oszt.
- **F-DC:** bizalmas adatokat feldolgozó rendszerek osztálya.
- **F-DX:** magas adat-integritást és bizalmasságot biztosító osztott rendszerek osztálya.

CC

- **CC** (**C**ommon **C**riteria = Közös Követelmények)

Az EU, az USA és Kanada együttműködésével jött létre azzal a céllal, hogy a korábbi ajánlásokat összhangba hozza a különböző alkalmazási területekre **egyedi követelményeket** szabjon.

ITIL

- **ITIL** (BS 15000:2000) Az Informatikai Szolgáltatás Módszertana.

Az ITIL-t jó minőségű, **költséghatékony** informatikai szolgáltatások támogatása céljából fejlesztették ki, mely kiterjed azok teljes életciklusára, így a tervezésre, bevezetésre, működtetésre és újabb szolgáltatások bevezetésére.

COBIT

- **COBIT** 4.1 Informatikai Irányítási és Ellenőrzési Módszertan.

Nemzetközileg elfogadott keretelv, amely garantálja az informatikai alkalmazásoknak az **üzleti célok** szolgálatába való állítását, **erőforrásaik** felelős felhasználását és a **kockázatok** megfelelő kezelését.

ISO/IEC

- ISO/IEC 27000

Nemzetközi Szabványügyi Szervezet (ISO) által is elfogadott és elismert ISO szabvány gyűjteménye.

INFOSEC

- **INFOSEC** (**I**nformation **S**ystem **S**ecurity **=** Informatikai Rendszerek Biztonsága)

A NATO információvédelmi ajánlása, amely szerint:

„Az információvédelem biztonsági intézkedések alkalmazása annak érdekében, hogy a kommunikációs, információs és más elektronikus rendszerekben tárolt, feldolgozott és átvitt adatok védelme biztosítva legyen a ***bizalmasság, sértetlenség és rendelkezésre állás*** *elvesztésével szemben, függetlenül az események szándékos vagy véletlen voltától*”.

INFOSEC két része:

- Communication Security (COMSEC)
  - CRYPTOSEC - rejtjelezés
  - TRANSEC – átviteli utak védelme
  - EMSEC – kompromittáló kisugárzás elleni védelem
- Computer Security (COMPUSEC)
  - Hardverbiztonság
  - Szoftverbiztonság
  - Firm-ware biztonság (csak olvasható memóriában tárolt adatok)

ITB

- **ITB** (Informatikai Tárcaközi bizottság)

A Miniszterelnöki Hivatal Informatikai Tárcaközi bizottsága által kiadott ajánlások az informatikai biztonság megteremtésének legfontosabb tudnivalóiról adnak tájékoztatást.

- **ITB 8. :** tartalmazza az informatikai biztonság kockázatelemzésének egy jól használható módszertanát.
- **ITB 12. :** az informatikai rendszerek biztonságának követelményeit tartalmazza.
- **ITB 16. :** az informatikai termékek és rendszerek biztonsági értékelésének módszertana.

Nemzetközi információbiztonsági szervezetek:

- **ENISA** Európai Hálózat- és Informatikai Biztonsági Ügynökség;
- **CERT**-ek Számítógépes Vészhelyzeti Reagáló Csoportok és
- **CSIRT**-k Számítógépes Biztonsági Incidens Reagáló Csoportok;
- **TF-CSIRT** az Európában működő CERT szervezetek közös szervezete;
- **FIRST** incidenskezelő szervezetek fóruma;
- **EGC** Európai kormányok CSIRT csoportja.

TEMPEST

A TEMPEST egy vizsgálat fedőneve volt, amely során a különböző elektronikai adatfeldolgozó egységek kisugárzását elemezték. Megállapították, hogy minden egy elektronikai berendezés kibocsát rezgéseket, amelyeket elfogva, és különböző eljárásoknak alávetve, az adatok kinyerhetőek.

A tökéletes információ védelmet csak a fizikai közeg átalakítása, valamint a háttérzaj létrehozásával érhetik el.

A TEMPEST jelzést gyakran használják, illetve említik úgy hogy **Kisugárzás Biztonság vagy Biztonságos Sugárzás** (EMSEC – avagy sugárzás biztonságtechnika).

USA és a NATO TEMPEST szintjei

NATO SDIP-27 A Szint (régebben AMSG 720B) és az USA-ban NSTISSAM Szint I
„Egyezményes Laboratóriumi Test Kisugárzási szint”
Ez a „stricteszt” mondhatni rövidtávú szint, azon egységeknek feleltethető meg, ahol az információ elnyelő, nevezzük támadónak, szinte közvetlenül hozzáfér az adatokhoz, azaz a kisugárzást közvetlen közelről rögzíti. (maximum 1méteres távolságig megengedett ezen szintben a támadó) NATO Zóna 1 szint
NATO SDIP-27 B Szint (régebben AMSG 788A) és az USA-ban USA NSTISSAM Szint II
"Laboratóriumi Próba Szabvány Gyengén Védett Berendezésekre"
Ez egy némileg lazább szabvány, ami NATO Zóna 1 egységeknél az működik. A szabvány szerint adott egy támadó, aki a kisugárzó berendezéshez maximum 20 méteres távolságba tud csak közel jutni. A szabvány szerint a támadó számára fizikai kontaktus lehetetlen. (a 20 méteres táv mérésében, fizikai közeg nem játszik szerepet, így az építőanyagok, vagy páncélzat sem)
NATO SDIP-27 C Szint (régebben AMSG 784) és az USA-ban NSTISSAM Szint III
"Labor Próba Szabvány, Taktikai Mobil Berendezés / Rendszerek "
Ez a szint, még inkább lazább szabvány, amely NATO Zóna 2 egységekben működik. A szabványban a támadó maximum 100 méterre tudja megközelíteni a kisugárzás forrását.