Miloszlike törölve dr. Lamperth Mónika
bm 33-17611/2005, rend. alapj. 2005. 11. 04-e

BELÜGYMINISZTÉRIUM

TITKOS!

Szám: 10—21/9/1983.

№ 240

A MAGYAR NÉPKÖZTÁRSASÁG BELÜGYMINISZTERÉNEK 9/1983. számú UTASÍTÁSA

Budapest, 1983. évi május hó 9-én.

BELÜGYMINISZTÉRIUM

TITKOS!

Szám: 10—21/9/1983.

A MAGYAR NÉPKÖZTÁRSASÁG BELÜGYMINISZTERÉNEK 9/1983. számú UTASÍTÁSA

a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről

Budapest, 1983. évi május hó 9-én.

A számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről szóló 1/1981. (I. 27.) BM számú rendelet végrehajtására kiadom az alábbi

u t a s í t á s t :

1. Az utasítás hatálya kiterjed:

   a) a Belügyminisztériumban és szerveinél működő, operációs rendszerrel (felügyelő-, kezelőprogramokkal) ellátható számítástechnikai eszközökre (a továbbiakban: számítógép), a számítógépek közeli és távoli termináljaira, az adatelőkészítő berendezésekre;

   b) arra a szervre, amelynél az a) alpontban felsorolt valamely eszköz rendszeresítve van vagy ilyen eszköz működik, (a továbbiakban: üzemeltető) illetve ezek szolgáltatásait igénybe vevő szervre;

   c) az üzemeltetéshez és feldolgozáshoz szükséges programokra, adatállományokra, valamint ezek adathordozóira;

   d) a számítástechnika — alkalmazás teljes folyamatára.

2. A Belügyminisztériumban és szerveinél működő minden számítógép — a 3. és 4. pontban meghatározottak kivételével — a fokozott biztonság kategóriájába tartozik.

3. Az illetékes miniszterhelyettes vagy a belügyminisztériumi államtitkár az üzemeltető szerv parancsnokának előterjesztése alapján engedélyezheti a számítógép alapbiztonsági kategóriába való sorolását, ha a működtetés körülményei nem teszik indokolttá a fokozott biztonság kategóriájára vonatkozó intézkedések megtételét.

4. Kiemelt biztonsági kategóriába tartoznak a belügyminisztériumi államtitkár vagy az illetékes miniszterhelyettes által kijelölt számítógépek. Az ilyen számítógépekkel ellátott számítóközpontban — a titokvédelem és az 1/a. alpontban felsorolt eszközök védelme szempontjából indokolt területen — az általánosnál szigorúbb kiegészítő biztonsági előírásokat kell rendszeresíteni.

5. Az utasítás hatálybalépésekor üzemelő számítógépek kategóriába sorolását 1983. december 31-ig végre kell hajtani. Az ezt követő időszakban a Belügyminisztériumban és szerveinél üzembe helyezésre kerülő számítógépeknél a rangsorolást már a tervezés időszakában végre kell hajtani.

6. A fokozott és a kiemelt biztonsági kategóriába tartozó számítógépeknél a BM III. Főcsoportfőnökség illetékes szerve 1984. június 30-ig:

   a) mérje fel és határozza meg az elektromágneses ki- és besugárzás elleni védelemre, valamint a hasznos információk akusztikusan, elektromos tápfeszültségű, világítási és nemkívánatosan a hírközlő hálózatokon való kijutás elleni technikai védelemre vonatkozó műszaki normatívákat és mérési módszereket.

   b) dolgozzon ki a biztonsági fokozatnak megfelelő védelem létesítéséhez, ellenőrzéséhez és folyamatos biztosításához szükséges technikai, anyagi, pénzügyi feltételeire vonatkozóan — a BM I. Főcsoportfőnökség illetékes szerveivel egyeztetett — javaslatot.

7. A BM III. Főcsoportfőnökség illetékes szerve rendszeresen ellenőrizze a kisugárzás mértékét, információtartalmát vala-

mennyi, az utasítás hatálya alá tartozó számítógépnél. Az ellenőrzés során feltárt hiányosságok megszüntetéséről az üzemeltető szerv parancsnokának gondoskodni kell.

8. A fokozott és a kiemelt biztonsági kategóriába sorolt számítógépeknél az elektromágneses ki- és besugárzás elleni védelem, valamint a hasznos információk akusztikus úton, elektromos tápfeszültségű, világítási hálózaton és nemkívánatosan a hírközlő hálózatokon való kijutás elleni védelem biztosításáért felelős az üzemeltető szerv vezetője.

9. Az üzemeltető szerv parancsnoka felelős azért, hogy minden számítógép, terminál és adatelőkészítő berendezés telepítése, üzemeltetése a biztonsági szabályok figyelembevételével történjék, azok betartását köteles rendszeresen ellenőrizni.

10. Az üzemeltető szerv parancsnoka felelős azért, hogy a számítógép biztonsági kategóriájának megváltozása esetén ideiglenes intézkedésekkel biztosítsa a megfelelő védelmet arra az átmeneti időszakra, amely a fokozatnak megfelelő végleges védelmi intézkedések megtételéhez és a 40. pontban meghatározott számítástechnikai védelmi szabályzat módosításához szükséges.

11. Államtitkot vagy szolgálati titkot tartalmazó (a továbbiakban együtt: minősített) gépi adathordozókat a 3/1971. (IX. 23.) BM számú rendelettel kiadott, az államtitok és szolgálati titok védelmének eljárási szabályzata, az adott szervre vonatkozó ügykezelési (iratkezelési) szabályzat és a BM Titkárság vezetőjének 1/1976. számú Elvi Állásfoglalása (a továbbiakban együtt: TÜK szabályok) rendelkezéseivel összhangban és az 1/1981. (I. 27.) BM számú rendelet, valamint a Központi Statisztikai Hivatal elnöke által kiadott irányelvek (a továbbiakban: Irányelvek) figyelembevételével kell kezelni.

12. A nem minősített gépi adathordozókat (pl. programokat, próbaadatokat stb. tartalmazó adathordozók) szolgálati helyen kívül tárolni, tanulmányozni vagy felhasználni nem szabad. E rendelkezés alól az üzemeltető szerv parancsnoka egyedi esetben írásban felmentést adhat.

13. Titkos adatokat felhasználó, vagy előállító feldolgozást csak a TÜK szabályok szerint és dokumentációk alapján lehet folytatni.

14. A kiemelt biztonság kategóriájába tartozó számítógépet, annak titkos adatok forgalmazását és rögzítését ellátó közeli és távoli termináljait, adatelőkészítő berendezéseit elektromágneses árnyékoló rendszerrel kell ellátni.

15. Minősített adathordozók szállításánál a TÜK szabályok szerint kell eljárni.

16. Mágneses adathordozót csak zárt fémborítású, a káros rázkódások és elektromágneses besugárzások ellen védő csomagolásban, a 15. pontban foglaltak betartásával lehet szállítani. A mágneses adathordozók szállítását, ha a küldemény súlya és terjedelme szükségessé teszi, az üzemeltető szerv parancsnoka által kijelölt külön futár végzi.

17. A számítógéppel végzett feldolgozás védelme attól függ, hogy nem titkos, illetőleg titkos adatokat felhasználó vagy előállító feldolgozás folyik.

18. A fokozott biztonság kategóriájába tartozó számítógépek géptermébe, illetve a kiemelt biztonság kategóriájába tartozó számítógéppel ellátott számítóközpontba csak az arra rendszeresített, külön belépési engedéllyel lehet belépni.

19. Aki nem tartozik az üzemeltető szerv állományába, a számító- (adatrögzítő-) gépteremben csak akkor tartózkodhat, ha a számítógépen nem folyik titkos adatokat felhasználó vagy előállító feldolgozás és a belépésre írásban engedélyt kapott. Indokolt esetben a feldolgozás ideje alatt ott-tartózkodásra írásban külön engedély adható.

20. Szolgálati titkot képező adatot felhasználó vagy előállító feldolgozás esetén a számító (adatrögzítő-) gépteremben csak a jóváhagyott dokumentációban felsorolt, valamint az arra rendszeresített belépési engedéllyel rendelkező személy tartózkodhat.

21. Ha a feldolgozás államtitkot képező adatokat használ fel vagy állít elő, akkor a számító- (adatrögzítő-) gépteremben

csak a jóváhagyott dokumentációban név és beosztás szerint megnevezett személy tartózkodhat. Ettől való eltérést csak a dokumentációt jóváhagyó vagy annak elöljáró parancsnoka engedélyezhet írásban. A gépteremben tartózkodásra ilyen esetben a belépési engedély önmagában nem jogosít.

22. A számító- (adatrögzítő-) gépterembe belépőkről nyilvántartást kell vezetni.

23. A számítógépen végzett karbantartási munkáról nyilvántartást kell vezetni. A nyilvántartás tartalmazza a munkát végzők és a munkánál jelen levők azonosítására alkalmas adatokat és tegye lehetővé a javítás során esetleg kicserélt alkatrészek további útjának figyelemmel kísérését.

24. A számítógépet üzemeltető szerv vezetője az adatok pótlása érdekében másodlagos adattár létesítéséről köteles gondoskodni.

25. A másodlagos adattárat a számítógéptől távol, más épületben kell elhelyezni.

26. Gondoskodni kell a másodlagos adattár ellenőrzéséről, felfrissítéséről és naprakész állapotban tartásáról.

27. A számítógép operációs rendszere és a rendszerkomponensek a pótolhatatlan adatállomány kategóriájába tartoznak. Gondoskodni kell a másodlagos adattárakat kezelő, feldolgozó programok és operációs rendszer olyan állapotban tartásáról, hogy a másodlagos adattárak felhasználása a háttér számítógépen is biztosított legyen.

28. A kihelyezett képernyős terminálon megjelenő szöveg minősítésének megfelelő iratnak minősül. A betekintés engedélyezésénél a TÜK szabályok szerint kell eljárni.

29. A kihelyezett terminálon megjelenített adatok titokvédelméért, illetve a titok megőrzését biztosító feltételek megteremtéséért, a védelemre vonatkozó előírások betartásáért a terminált üzemeltető szerv parancsnoka felelős.

30. Ha a kihelyezett terminál helyi feldolgozásra is alkalmas, akkor az utasítás alkalmazásában számítógépnek minősül.

31. A számítástechnikai eszközökhöz kapcsolódó adatátviteli csatornákon titkos adatok forgalmazása a 36. pontban megha-

tározottak alkalmazása nélkül — a 32. pontban foglaltak kivételével — tilos.

32. Rejtjelző berendezés alkalmazása nélkül is forgalmazhatók titkos adatok, ha az adatátviteli csatorna nem hagyja el az ellenőrzött területet, és emellett az általa kibocsátott sugárzás más vezetékeken való kijutása, a csatornák téves összekapcsolása és az adatátviteli csatornákon folyó információk egyéb módon történő kijutása kizárt, és ezek alapján arra a belügyminisztériumi államtitkár vagy az illetékes miniszterhelyettes írásban engedélyt adott.

33. Ellenőrzött területnek az a terület minősül, amelyen a rendszeresített berendezési tárgyakon kívül idegen technikai és szállítóeszközök, egyéb tárgyak, továbbá idegen személyek engedély nélküli jelenléte kizárt.

34. Az ellenőrzött területen külföldi állampolgárok nem tartózkodhatnak. Ha ott-tartózkodásuk elkerülhetetlen, jelenlétük ideje alatt titkos adatokat nem lehet feldolgozni, kivéve ha arra a belügyminisztériumi államtitkár vagy az illetékes miniszterhelyettes írásban engedélyt adott.

35. Ha az ellenőrzött területen a rendszeresített berendezési tárgyakon kívül más tárgy is van, titkos adatot nem lehet feldolgozni.

36. Ha az adatátviteli csatorna elhagyja az ellenőrzött területet, titkos adatok forgalmazása csak az Országos Rejtjelközpont által rendszeresített rejtjelző berendezésen keresztül a hatályos jogszabály, belügyi rendelkezés szerint történhet.

37. A számítástechnikai rendszerek tűzvédelmét az 1/1981. (I. 27.) BM számú rendelet 19. §-a és a Belügyminisztériumra és szerveire irányadó tűzvédelmi rendelkezések szerint kell megszervezni.

38. Az üzemeltető szerv parancsnoka köteles gondoskodni arról, hogy számítástechnikai rendszerek tervezése és létesítése (bővítése, átalakítása és felújítása), a számítóközpont tűzoltókészülékekkel való ellátása, a tűzvédelmi előírások szabályai szerint történjék.

39. A fokozott biztonság kategóriájába tartozó számítógépek esetében ajánlott, a kiemelt biztonsági kategóriába sorolt szá-

mítógépek esetében pedig kötelező a tűz-, füst-, behatolás-, víz-, betörés-, hőmérséklet- és páratartalomjelző készülék telepítése.

40. A számítógépet üzemeltető szerv parancsnoka 1984. június 30-ig vagy az új számítógép üzembehelyezését követő 6 hónapon belül a számítógép biztonsági kategóriájának megfelelő számítástechnikai védelmi szabályzatot (a továbbiakban: SZVSZ) köteles készíteni és azt naprakész állapotban tartani. Az SZVSZ-t kiadása előtt egyeztetni kell a BM III/II. csoportfőnökkel, a BM országos rendőr-főkapitány bűnügyi helyettesével és a BM Tűzoltóság országos parancsnokával.

41. A SZVSZ-t az Irányelvek 24—26. pontja, valamint az utasítás alapján az érintett szerv sajátosságainak megfelelően kell elkészíteni.

42. A kiemelt biztonsági kategóriába sorolt számítóközpontot ért katasztrófa hatásának mérséklése, valamint a gyors helyreállítás érdekében a számítógépet üzemeltető szerv parancsnokának a rendkívüli időszakra vonatkozó rendelkezésekkel, illetőleg a szerv „M" tervével összhangban az SZVSZ részét képező katasztrófa-tervet kell készíteni.

43. A katasztrófa-terv tartalmazza:

a) a katasztrófa bekövetkezése utáni teendőket,

b) a mentési és helyreállítási feladatokat,

c) a háttérgép kijelölését,

d) a legalapvetőbb tevékenységi kör kijelölését,

e) a munka folytatásának feltételeit,

f) a munka folytatásának módját,

g) az áttelepítési tervet.

44. A katasztrófa-terv melléklete tartalmazza a munka folytatásához szükséges adatállományok besorolását annak megfelelően, hogy azok néhány nap vagy néhány hónap alatt pótolható vagy pótolhatatlan adatok.

45. A katasztrófa-tervben szereplő háttérgépet a belügyminisztériumi államtitkár vagy az illetékes miniszterhelyettes je-

ÁBTL - 4.2 - 10 - 21/9/1983 /8

löli ki a szerv „M" tervében meghatározottakkal összhangban.

46. A 42., 43., 44., 45. pont alkalmazásában katasztrófa: a számítástechnikai eszközök vagy adathordozók elemi csapás következtében bekövetkezett részleges vagy teljes megsemmisülése, amely a feldolgozást a legalapvetőbb tevékenységi körben lehetetlenné teszi.

47. A számítógépet üzemeltető szerv parancsnoka adatvédelmi felelőst vagy — a szerv sajátosságainak megfelelően — adatvédelmi felelősöket jelöl ki. Adatvédelmi felelősnek csak olyan beosztásban levő jelölhető ki, amelyben adatvédelmi kérdésekben a napi munka szintjén dönteni, intézkedni nem kell. Az adatvédelmi felelős közvetlenül a parancsnoknak van alárendelve.

48. Az adatvédelmi felelős jogait és kötelezettségeit — a belügyminisztériumi államtitkár vagy az illetékes miniszterhelyettes egyetértését követően —, az Irányelvek 27—28. pontja alapján az SZVSZ mellékletében kell megállapítani és azt a munkaköri leírásban is rögzíteni kell.

49. A belügyminisztériumi államtitkár az állambiztonsági miniszterhelyettes javaslatára az adatvédelmi felelősök szakirányítása céljából felügyeleti adatvédelmi felelőst jelöljön ki.

50. Az utasításban nem szabályozott kérdésekben a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről szóló 1/1981. (I. 27.) BM számú rendelet szabályait, valamint az Irányelveket kell alkalmazni.

51. A belügyminisztériumi államtitkár vagy az illetékes miniszterhelyettes az anyagi és technikai feltételekkel összhangban engedélyezheti:

    a) az üzemeltető szerv parancsnokának előterjesztése alapján a Belügyminisztérium illetékes szervével történt előzetes véleményezést követően a tűz-, füst-, behatolás-, víz-, betörés-, hőmérséklet- és páratartalomjelző készülék telepítésének;

    b) az utasítás hatálybalépésekor már telepített számítógépek elektromágneses kisugárzás elleni védelme kiépítésének;

c) a másodlagos adattárak elhelyezésére vonatkozó kötelezettség

elhalasztását — a magasabb biztonsági kategóriába való kerülés esetében is —, ha egyéb módon is hatékonyan biztosítható a titok-, vagyon- és tűzvédelem.

52. Ez az utasítás kiadása napján lép hatályba, rendelkezéseit az érintett állománnyal ismertetni kell.

Dr. HORVÁTH ISTVÁN s. k.,
belügyminiszter

FÜGGELÉK

Készült: 260 példányban.
Kapják: államtitkár,
miniszterhelyettesek,
főcsoportfőnök-helyettesek,
országos parancsnokok, helyetteseik,
csoportfőnökök, helyetteseik,
önálló és beosztott osztályvezetők,
BM iskolák parancsnokai,
budapesti, megyei rendőr-főkapitányok,
Hőr. ezred-, ill. kerületparancsnokok.

FÜGGELÉK

A MAGYAR NÉPKÖZTÁRSASÁG BELÜGYMINISZTERÉNEK 1/1981. (I. 27.) BM számú RENDELETE

a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről

A Minisztertanács felhatalmazása alapján — a Központi Statisztikai Hivatal elnökével, valamint az érdekelt miniszterekkel és országos hatáskörű szervek vezetőivel egyetértésben — a következőket rendelem:

Általános rendelkezések

1. §

(1) E rendelet hatálya kiterjed:

a) a számítógépet és egyéb számítástechnikai berendezést birtokban tartó, üzemeltető vagy számítógépes adatfeldolgozást végző (a továbbiakban: üzemeltető), annak működését megrendelő vagy igénybe vevő (a továbbiakban: felhasználó) valamenynyi állami szervre, szövetkezetre, állami feladatot ellátó társadalmi szervezetre, valamint egyesületre (a továbbiakban: szerv);

b) a számítástechnikai rendszerben feldolgozás alatt levő és ott tárolt, illetve a feldolgozás eredményeképpen létrejött, az a) pontban meghatározott szerv ügykörébe tartozó minden, valamint a személyhez fűződő jogokkal kapcsolatban meghatározott iratra vagy adatra (a továbbiakban: adat) illetve adathordozóra, függetlenül annak feldolgozási vagy előállítási módjától és megjelenési formájától;

c) a számítástechnika-alkalmazás teljes folyamatára.

(2) E rendelet alkalmazásában:

a) számítógép és egyéb számítástechnikai berendezés (a továbbiakban: számítástechnikai berendezés) minden olyan gépi berendezés és eszköz, amely az (1) bekezdés b) pontjában meghatározott adat előállításában, feldolgozásában, tárolásában, továbbításában és megjelenítésében részt vesz;

b) számítástechnika-alkalmazás folyamatán a számítástechnikai berendezések üzemeltetése, az alap- és rendszerprogramok, alkalmazási programok és azok dokumentációinak előkészítési, tervezési, megvalósítási, működési és fejlesztési szakaszai, illetve az ezek alapját képező megrendelések (szerződések), valamint az adathordozók tárolása és felhasználása értendők.

2. §

(1) A fegyveres erők és a fegyveres testületek, illetve az e szerveket érintő adatok feldolgozása vonatkozásában az illetékes miniszter, valamint a Munkásőrség országos parancsnoka — a belügyminiszterrel egyetértésben — az e rendeletben foglaltaktól eltérő szabályokat is megállapíthat.

(2) E rendelet nem érinti az állami népességnyilvántartás rendszerében történő adatszolgáltatásról szóló 6/1979. (X. 24.) BM—HM—IM számú együttes rendelet, valamint a statisztikai adatok elektronikus gépi úton történő feldolgozásáról és tárolásáról szóló 2/1977. (VII. 30.) KSH számú rendelkezés hatályát.

A védelem tárgya és eszközei

3. §

(1) A számítástechnika-alkalmazás folyamatában és annak szakaszaiban a védelem tárgya:

a) az adatok és azok hordozói végleges megsemmisítésükig, a közlésre szánt adatok a felhasználásukig;

b) a személyhez fűződő és a vagyoni jogok;

c) a számítástechnikai berendezések, azok környezete, működésük biztonsága és a dokumentációik;

d) a számítástechnikai berendezésekhez tartozó okmányok, programok és azok dokumentációi;

e) az alkalmazott biztonsági intézkedések, azok tervei, tartalmi előírásai és eljárási szabályai.

(2) Védelmi eszköznek minősül mindaz a műszaki, technológiai, programozási, szervezési és jogi intézkedés és eszköz, amely a védelem tárgyát a veszélyforrás ellen biztosítja.

(3) Kiegészítő biztonsági intézkedés a titkot képező adatok megőrzését szolgáló szigorító vagy különleges védelmi eszköz.

A védelmi eszközök alkalmazása

4. §

(1) A számítástechnika-alkalmazás folyamatában részt vevő szervek vezetői felelősek a hatáskörükbe tartozó — a számítástechnikai biztonság megteremtéséhez szükséges — intézkedések, illetve védelmi eszközök meghatározásáért és alkalmazásuk feltételeinek biztosításáért.

(2) A számítástechnika-alkalmazás folyamatának bármely szakaszában szükséges kiegészítő biztonsági intézkedést, valamint az ezzel kapcsolatos jogokat és kötelességeket — eltérő rendelkezés hiányában — az e tevékenységben részt vevő szervek vezetői közösen állapítják meg és a szerződésben rögzítik. Ez nem érinti a titkok védelmével kapcsolatos személyi felelősséget.

(3) A (2) bekezdés szerinti kiegészítő biztonsági intézkedést az a szerv köteles alkalmazni, amelynek érdekkörében az felmerül. Ez az irányadó a kiegészítő biztonsági intézkedés alkalmazása költségfedezetének viselésére is.

5. §

(1) A számítástechnika-alkalmazás folyamatában érdekelt üzemeltető szervek felügyeletét ellátó, ennek hiányában az ágazatilag illetékes miniszter, illetőleg országos hatáskörű szerv ve-

ÁBTL - 4.2 - 10 - 21/9/1983 /14

zetője (a továbbiakban: felügyeletet ellátó miniszter) e rendelet végrehajtására — a belügyminiszterrel és a Központi Statisztikai Hivatal elnökével egyetértésben — területe sajátosságainak megfelelő utasítást ad ki.

(2) Az utasítás kiterjed:

a) a számítástechnikai berendezések biztonsági követelményeknek megfelelő üzemeltetésére és az általános adatvédelmi előírásokra;

b) a titokvédelmet szolgáló kiegészítő biztonsági intézkedések alkalmazásának szükségességére, módjára és mértékére;

c) a különleges tűz- és vagyonvédelmi feladatokra;

d) a kötelező biztonsági jelző- és riasztóberendezések alkalmazására;

e) a távadatfeldolgozás alkalmazásának biztonsági feltételeire és a nemzetközi adatátvitel eljárási rendjére;

f) a tárgyi feltételekre és a személyi felelősségre;

g) a számítástechnikai védelmi szabályzat kiadásának rendjére.

6. §

A számítástechnikai rendszer részletes titok-, vagyon- és tűzvédelmi feladatait az üzemeltető szerv vezetője számítástechnikai védelmi szabályzatban határozza meg.

Titkot képező adatok védelme

7. §

(1) Államtitoknak, illetőleg szolgálati titoknak minősülő adatot csak a védelméhez szükséges kiegészítő biztonsági intézkedések megléte, illetve megtétele esetén lehet számítástechnikai rendszerben feldolgozni. Ez vonatkozik a feldolgozás folyamatában titokká váló adatokra is.

(2) Államtitoknak minősülő adat számítógépes feldolgozásához — eltérő rendelkezés hiányában — a felhasználó szerv

vezetője adhat engedélyt. Az engedélyt — a feldolgozás feltételeinek egyidejű meghatározásával — írásban kell megadni.

(3) Szolgálati titoknak minősülő adat számítógépes feldolgozásához az (1) bekezdésben írt feltételek megléte esetén a felhasználó szerv illetékes minősítője adhat meghatározatlan időre szóló engedélyt. Az engedélyt — a feldolgozás feltételeinek egyidejű meghatározásával — írásban kell megadni.

8. §

(1) A számítástechnikai védelmi szabályzatban az államtitoknak és a szolgálati titoknak minősülő adatok számítógépes rendszerben történő feldolgozása teljes technológiai folyamatát szabályozni kell. Meg kell határozni:

a) a nyilvántartási tevékenység szabályait és eszközeit;

b) az adatok bizonylatait és azok áramlásának útját;

c) az adatok feldolgozási folyamatát és védelmük módját;

d) az adattárolás és az adatkibocsátás (továbbítás) rendjét;

e) a feleslegessé vált vagy hibás adatok (adathordozók) selejtezési és megsemmisítési rendjét;

f) a betekintési jogosultságot;

g) az ellenőrzési jogokat és kötelezettségeket.

(2) A bizonylatok kódolására szolgáló kódjegyzék, a szervezési — indokolt esetben — a programozási és üzemeltetési dokumentáció az adatok jellegének megfelelően minősül.

9. §

(1) Titoknak minősülő és titkot nem képező adatokat a gépegységeken egyidejűleg feldolgozni csak az operációs és az adatbázis kezelő rendszerben kialakított biztonságos technikai megoldások alkalmazásával lehet.

(2) A különböző minősítésű programok egyidejű futtatásának biztonságos megszervezéséért és az illetéktelen hozzáférés megakadályozásáért az üzemeltető szerv vezetője felelős.

(3) Ha a számítógépes feldolgozás során a titkot nem képező alap- (elsődleges) adatok összesítésük, összefüggéseik révén államtitokká vagy szolgálati titokká válnak vagy eltérő minősítésű és nyílt adatok együttes feldolgozása történik, azokat a jellegüknek megfelelően minősíteni kell. Ez értelemszerűen vonatkozik a feldolgozás dokumentációjára is.

10. §

(1) Az államtitkot vagy szolgálati titkot tartalmazó adathordozót megfelelő minősítési jelöléssel kell ellátni oly módon, hogy az a feldolgozás egész folyamatában azonosítható és értelmezhető legyen. Ezt az eljárást kell alkalmazni a másolások során újraelőállított valamennyi minősített adathordozóra is.

(2) Annak érdekében, hogy az adathordozó nyilvántartása és kezelése során a titok jellege egyértelműen kitűnjön, az azonosításhoz szükséges adatot és más kezelési előírást, az adathordozóval azonos minősítésű kísérőlapon kell feltüntetni.

(3) A programozási dokumentációval együtt átadott másodlagos, kódolt bizonylaton a minősítési jelölést a bizonylatot kiállító szerv tünteti fel.

(4) Az államtitoknak minősülő adatok kódolására, rejtjelzésére használt eszközök, konzolpapírok és az alkalmazott bizonylatok kezelésénél és őrzésénél a titkos ügykezelés (a továbbiakban: TÜK) előírásainak megfelelően kell eljárni.

11. §

A titkot képező adatok védelmét — a feldolgozás, az adattovábbítás és a tárolás során — az operációs rendszerben és a programrendszerekben alkalmazott logikai-matematikai, illetve a berendezésekben alkalmazott megfelelő technikai megoldásokkal is biztosítani kell (software, illetve hardware adatvédelem).

12. §

(1) A minősített adatokat feldolgozó, létrehozó számítógépes adatfeldolgozó rendszer rendszerdokumentációjának tartalmaznia kell az adatállomány megőrzésének és felülírásának szabá-

lyait, technológiáját, valamint az adatállomány megsemmisítésére szolgáló fizikai törlő program leírását.

(2) Megőrzés vagy felülírás esetén a rendszerdokumentációban foglaltak szerint kell eljárni.

(3) A titkot képező mágneses adathordozón tárolt adatok fizikai törlése megsemmisítésnek minősül.

(4) Minősített adatokat tartalmazó adathordozó meghibásodása vagy megrongálódása esetén az adathordozót

— a fizikai törlő program alkalmazásával törölni kell vagy

— az indokolt terjedelemben fizikailag meg kell semmísíteni.

(5) A törlő program alkalmazásáról jegyzőkönyvet kell felvenni.

(6) Vizuálisan olvasható adathordozón tárolt, a számítástechnikai eszköz vagy a számítógépes adatfeldogozó rendszer téves működése miatt hibássá vált titkot képező adatot, a minősített adathordozókkal együtt kell tárolni, majd selejtezni kell és meg kell semmisíteni.

13. §

(1) A betekintési jogosultságot és az annak gyakorlását biztosító jelszavak, kulcsok és más eszközök körét az adatfeldolgozásban részt vevő személyekre munkakörönként és a mindenkori feldolgozási üzemmód figyelembe vételével — írásban — kell meghatározni.

(2) A betekintési jogosultság meghatározásának arra is ki kell terjednie, hogy a titoknak minősülő adatokhoz ki és milyen feltételek mellett illetékes hozzáférni.

(3) A kijelölt dolgozók előtt a titokvédelmi és egyéb rendszabályokat, valamint a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell. Ennek tudomásulvételét írásbeli nyilatkozatba kell foglalni, és erről nyilvántartást kell vezetni.

(4) A titkot képező tárolt adatok jegyzékét, a mindenkori jelszavak és kulcsszavak jegyzékét, valamint az azokat igénybe

vevők és a betekintők névsorát a TÜK szabályai szerint kell kezelni.

14. §

(1) Az államtitkot tartalmazó adathordozók tárolásánál a TÜK előírásainak megfelelően kell eljárni.

(2) A titkot tartalmazó adatok biztonsági okokból előállított másolati adathordozóit (másodpéldányokat) más épületben és lehetőleg területileg is távol, biztonságos körülmények között kell tárolni.

15. §

(1) A titkot tartalmazó adathordozó szállítását úgy kell előkészíteni, hogy azt a szállítás közben károsodás ne érje, illetéktelenek hozzá ne férjenek.

(2) A titkot tartalmazó mágneses adathordozót az elektromágneses zavaró hatás ellen védeni kell.

16. §

(1) A távadatfeldolgozás során az államtitok és a szolgálati titok megőrzését kiegészítő biztonsági intézkedésekkel kell biztosítani.

a) Államtitkot mind belföldön, mind külföldre, illetőleg szolgálati titkot külföldre hírközlő eszközön csak rejtjelezve lehet továbbítani:

— a rejtjelző eszközök és módszerek rendszerbe állításához a Belügyminisztérium illetékes szervének előzetes engedélye szükséges;

— a rejtjelző eszközök, módszerek meglétéről, szakszerű használatáról a számítástechnikai berendezést üzemeltető szerv köteles gondoskodni.

b) Az államtitok feldolgozására alkalmazott terminálokat (adatállomásokat) — titokvédelmi szempontból — a számítógépre vonatkozó biztonsági előírásoknak megfelelően kell telepíteni és üzemeltetni, függetlenül azok telepítési helyétől, illetve üzemeltetési módjától.

c) A szolgálati titokhoz való illetéktelen hozzáférést a távadatfeldolgozási környezetben különböző azonosító tárgyak, jelszó-listák felhasználásával, zavaró jelek közbeiktatásával, illetve szigorító biztonsági intézkedések alkalmazásával kell megakadályozni.

d) Az azonosító tárgyak, eszközök, valamint a terminál biztonságos őrzéséről — eltérő megállapodás hiányában — az üzemeltető köteles gondoskodni.

(2) Nemzetközi adatátvitel esetén:

a) államtitok, illetve szolgálati titok tekintetében a 14/1971. (IV. 15.) Korm. sz. rendelet 7. §-ában meghatározott engedély, egyéb adatok tekintetében a felhasználó szerv vezetőjének engedélye szükséges;

b) az adatátvitelről a Belügyminisztérium Titkárságát — államtitok, illetve szolgálati titok esetén előzetesen — tájékoztatni kell.

17. §

(1) A fontos államtitkok feldolgozásával rendszeresen foglalkozó számítástechnikai berendezések telepítésénél és üzemeltetésénél:

a) meg kell akadályozni az államtitkot képező adatoknak a telepítés helyéről elektromágneses kisugárzás útján, illetve vezetékeken történő kijutását;

b) el kell kerülni a nagy teljesítmény-szintű elektromágneses térerő jelenlétét.

(2) A zavaró szintű külső, és a számítógép egyes elemei által kisugárzott elektromágneses jelek jelenlétét, valamint a telepítési helyhez csatlakozó valamennyi vezetéket rendszeresen ellenőrizni kell.

(3) A felügyeletet ellátó miniszter által kijelölt számítóközpontot, illetve ennek számítástechnikai berendezéseit az egyedi vizsgálatoknak megfelelő indokoltság szerint védeni kell:

a) az adatokat kisugárzó vagy az elektromágneses térerőre érzékeny berendezéseket rádiófrekvenciás védő árnyékolással ellátott helyiségben kell elhelyezni;

ÁBTL - 4.2 - 10 - 21/9/1983 /20

b) a zavaró szintű külső környezeti hatások elkerülésére zaj- és rezgésszigetelést;

c) az adatok elektromos vezetés útján történő kijutásának megakadályozása érdekében megfelelő szűrést, illetve árnyékolást kell alkalmazni;

d) biztosítani kell a titkot képező adatok vizuális, illetve akusztikus kijutása elleni védelmet.

18. §

A számítástechnikai rendszerekben feldolgozott államtitok és szolgálati titok védelmére egyebekben a 3/1971. (IX. 23.) BM számú rendelet mellékleteként kiadott „Az államtitok és a szolgálati titok védelmének eljárási szabályzata" rendelkezéseit kell alkalmazni.

Vagyon- és tűzvédelem

19. §

(1) A számítástechnikai rendszerek általános vagyon- és tűzvédelmére

a) az Országos Építésügyi Szabályzat és

b) az Országos Tűzvédelmi Szabályzat előírásai, valamint

c) a BM Tűzoltóság Országos Parancsnokságának a számítóközpontok tűzvédelmére vonatkozó — MI—02102. számú — Műszaki Irányelvei érvényesek.

(2) A felügyeletet ellátó miniszter által megállapított nagyértékű, nagyteljesítményű vagy a különösen fontos államtitkok esetenkénti, illetve államtitkok rendszeres feldolgozására kijelölt számítóközpontot, illetve ennek számítástechnikai berendezéseit a káros külső környezeti hatásoktól — értéküknek és fontosságuknak megfelelően — fokozottabb védelemben kell részesíteni. Ennek során:

a) az esetleges veszély időbeni felismeréséhez megfelelő jelzőkészülékeket kell használni (tűz-, füst-, behatolás-, víz-, betörés-, hőmérséklet- és páratartalomjelző);

— A veszélyt jelző készülékeknek riasztórendszerbe való bekapcsolásáról gondoskodni kell. Törekedni kell a jelzés-átvi-

teli vezetékek védelmére, illetve nagy biztonságot nyújtó jelzésátviteli megoldások alkalmazására.

— A behatolást jelző készülékek riasztórendszerbe állítását a területileg illetékes rendőri szervvel előzetesen egyeztetni kell.

b) az őrzés megszervezése érdekében meg kell határozni:

— a megközelítés,

— a ki- és belépés,

— az ott-tartózkodás,

— az őrzés és a riasztás rendjét.

20. §

(1) Az elemi csapás okozta károk mérséklése, valamint a gyors helyreállítás érdekében — a 19. § (2) bekezdésében meghatározott számítóközpont esetén — áttelepítési, illetve a számítástechnikai védelmi szabályzat részeként katasztrófa-tervet kell készíteni.

(2) A katasztrófa-tervben kell meghatározni:

— a rendkívüli esemény bekövetkezése utáni teendőket;

— a mentési és a helyreállítási feladatokat;

— a folyamatos üzem biztosításához szükséges háttéreszközöket.

Személyhez fűződő jogok védelme

21. §

(1) Ha nem minősül államtitoknak, e rendelet alkalmazásában szolgálati titokként kell kezelni a természetes személyekre vonatkozó számítógépes nyilvántartást, feldolgozást és az ezek során keletkező adatot, kivéve azt, amelyet nyilvánosságra szántak, továbbá ha abból a természetes személyre nem lehet következtetni.

(2) A szervvel munkaviszonyban vagy munka végzésére irányuló egyéb jogviszonyban álló természtes személyekről számítógépes nyilvántartást, feldolgozást, adatelőállítást, adatközlést elrendelni csak a szerv rendeltetésszerű céljával összefüggésben és csak a szerv vezetőjének engedélyével lehet.

(3) A (2) bekezdés alá nem tartozó természetes személyre vonatkozó számítógépes nyilvántartást, feldolgozást, adatelőállítást, adatközlést elrendelni csak törvény, törvényerejű rendelet, minisztertanácsi rendelet és határozat alapján, a felhasználó szerv felügyeletét ellátó miniszter engedélyével lehet. Az engedélynek tartalmaznia kell az adatfelhasználás célját és a felhasználásra jogosultak körét.

Egyéb adatok védelme

22. §

Az államtitoknak vagy a szolgálati titoknak nem minősülő minden más adat védelmére — ideértve az üzemi titkot is — e rendeletet kell értelemszerűen alkalmazni, ha annak illetéktelen személy tudomására jutása valamely természtes vagy jogi személyre hátrányos következménnyel járhat.

23. §

A 22. §-ban meghatározott adatok védelmére vonatkozó eljárást, a védelem eszközeit, a biztonságos működés következményeinek megfelelően kell meghatározni.

Záró rendelkezések

24. §

(1) E rendelet következetes és szakszerű végrehajtása érdekében az üzemeltető, indokolt esetben a felügyeleti szervnél is megfelelő személyt kell megbízni (a továbbiakban: adatvédelmi felelős).

(2) Az adatvédelmi felelős a szerv vezetőjének megbízásából:

a) ellátja az adatfeldolgozás, valamint a számítástechnikai beruházások és új adatfeldolgozások szervezésének folyamatában a szakfelügyeletet;

b) gondoskodik a védelmi előírások megtartásának ellenőrzéséről a szükséges intézkedések kezdeményezéséről;

c) ellátja a titokvédelmi munka felügyeletét.

(3) Az adatvédelmi felelős jogait és kötelességeit az 5. §-ban meghatározott utasításban kell rögzíteni.

25. §

(1) A felügyeleti szerv ellenőrzi az e rendeletben foglaltak végrehajtását.

(2) Az üzemeltető, illetve a felhasználó szerv gondoskodik arról, hogy a számítástechnika-alkalmazás folyamatában államtitoknak minősülő adatok feldolgozásával csak politikailag és erkölcsileg megbízható személyek foglalkozzanak.

26. §

A Központi Statisztikai Hivatal:

a) e rendelet végrehajtását — a Belügyminisztériummal egyetértésben — számítástechnikai (szakmai) irányelvek kiadásával segíti elő;

b) lehetőséget biztosít a számítástechnikai adatvédelmi ismeretek egységes elvek és értelmezés szerinti elsajátításához.

27. §

(1) Ez a rendelet 1981. július 1-én lép hatályba.

(2) A felügyeletet ellátó miniszter a 16. § (1) bekezdésének a) pontjában, a 17. §-ában, valamint a 19. § (2) bekezdésének a) pontjában foglaltak végrehajtásának elhalasztását — az anyagi és technikai feltételekkel összhangban — a 7. § (1) és (2) bekezdésének figyelembevételével engedélyezheti.

Dr. HORVÁTH ISTVÁN s. k.,
belügyminiszter

A KÖZPONTI STATISZTIKAI HIVATAL ELNÖKÉNEK IRÁNYELVEI

a számítástechnikai rendszerek titok-, vagyon- és tűzvédelméről szóló 1/1981. (I. 27.) BM számú rendelet végrehajtásához

Az 1/1981. (I. 27.) BM számú rendelet (a továbbiakban: Rendelet) 26. §-a alapján, az 5. § és a 6. § egységes végrehajtása érdekében — a Belügyminisztériummal egyetértésben — az alábbi szakmai irányelveket állapítom meg:

Általános rendelkezések (alapelvek)

1. A számítástechnikai rendszerek titok-, vagyon- és tűzvédelmi feladatait,

a Rendelet előírásainak,

a jelen irányelvek elvárásainak,

az érintett jogszabályoknak,

a felügyeletet ellátó miniszterek által kiadott végrehajtási utasításoknak, valamint

a helyi adottságokat részletesen feldolgozó számítástechnikai védelmi szabályzatnak

egységes értelmezésével, összehangolt rendszerként kell megvalósítani.

ÁBTL - 4.2 - 10 - 21/9/1983 /25

A végrehajtást fentieken túlmenően a Központi Statisztikai Hivatal gondozásában megjelenő módszertani kézikönyv* és a KSH—SZÁMOK szervezésében lebonyolítandó speciális tanfolyamsorozat** segíti.

2. Amennyiben a Rendelet személyi vagy tárgyi hatálya által érintett területeken jogi személyiséggel nem rendelkező, de gazdasági-gazdálkodási (kisegítő) tevékenységet ellátó társulás vagy magánszemély végez munkát, vagy felhasználóként jelentkezik, ezekre nézve — az általános törvényi garanciákon túlmenően — a biztonsági feltételek meglétét kiemelten kell vizsgálni, és a szükséges előírásokat kétoldalú megállapodásban tételesen rögzíteni.

Titkot képező adatokkal történő munkavégzésbe, illetve szolgáltatásokba fenti személyek csak a minősítésre jogosult kifejezett ezirányú írásbeli felhatalmazása alapján vonhatók be.

3. A rendelet hatályával kapcsolatos vitás esetekben a felügyeletet ellátó miniszter állásfoglalása irányadó.

A védelem tárgya és eszközei. A védelmi eszközök alkalmazása

4. Veszélyforrásnak minősül bármely objektív esemény, tevés vagy mulasztás, amely a védelem tárgyát fenyegeti. A veszélyforrások körét a mindenkori műszaki-technikai fejlődés tükrében, az adott személyi és tárgyi környezetben kell vizsgálni, és folyamatosan figyelemmel kísérni.

A nem kötelezően kijelölt védelmi eszközöket a reálisan megállapítható vagy a körültekintő szakmai becslés alapján várható veszélyforrásokhoz kell hozzárendelni, a kockázat elemzési módszerek felhasználásával, és olyan módon, hogy azok a normál munkamenetet és a rendeltetésszerű használatot csak a szükséges minimumig korlátozzák.

---

* Megvásárolható a Statisztikai Kiadó Vállalat könyvesboltjában (Bp. II., Keleti Károly u. 10.)

** Jelentkezni lehet a KSH Nemzetközi Számítástechnikai Oktató és Tájékoztató Központ Oktatásszervezési Osztályán (1592 Budapest 112. Pf. 166).A tanfolyam díja személyenként 1300 forint.

5. Alapvető biztonsági intézkedésnek tekintendők mindazon műszaki, technológiai, programozási, szervezési és jogi eszközök, amelyek a rendeltetésszerű működés körében használatosak, és amelyek a Rendelet 22. §-ában meghatározott alapbiztonságot szolgálják, és nem minősülnek az alábbiak szerint kiegészítő biztonsági intézkedésnek.

Kiegészítő biztonsági intézkedésnek a Rendeletben a titkot képező adatok védelmével kapcsolatosan előírt számítástechnikai vonatkozású, valamint a 3/1971. (IX. 23.) BM számú rendeletben meghatározott, általános érvényű védelmi ügykezelési eljárások és eszközök, illetve a jelen Irányelvek 1. pontjában megjelölt források bármelyikében tételesen „kiegészítő biztonsági intézkedésnek" minősített védelmi eszköznek minősülnek.

6. A folyamatosan, tervezhető rendszerességgel, vagy előreláthatóan ismétlődően minősített (titkot képező) adatot feldolgozó, vagy felhasználó szervnél a kiegészítő biztonsági intézkedéseket (eszközöket) az alapvető biztonsági intézkedések rendszerébe építve és a számítástechnikai védelmi szabályzatba rögzítve kell tervezni, illetve alkalmazni. Ugyanezen előírás vonatkozik a felügyeletet ellátó miniszter által a Rendelet 17. § (3) bek. és a 19. § (2) bek. szerint kijelölt számítóközpontokra. Minősített adat eseti feldolgozása vagy felhasználása felmerülésekor, az ilyen jellegű tevékenységek folytatására előzetesen fel nem készült szervnél az adott munkafolyamatra a kiegészítő biztonsági intézkedéseket rendkívüli utasításban kell elrendelni, és azt — a számítástechnikai védelmi szabályzat külön kezelt és minősített részeként — megőrizni.

7. A számítástechnika-alkalmazás folyamatában több szerv együttes részvételével folyó tevékenységi keretnek tekintendők a főtevékenységként, vagy esetenként számítástechnikai szolgáltatást nyújtó szervek üzleti, üzemi, együttműködési kapcsolatai, a számítástechnikai szolgáltatások igénybevétele, azok eredményének felhasználása, az adat- vagy információszolgáltatást eredményező viszonylatok.

A Rendelet 4. §-ának alkalmazásában e szerveknek kell együttesen kialakítaniuk a megfelelő kiegészítő biztonsági intézkedéseket a szerződésben, illetve bármely más együttesen létrehozott és jóváhagyott dokumentumban, amely a közös működés feltételeit rögzíti.

ÁBTL - 4.2 - 10 - 21/9/1983 /27

A szerződést, illetve a fenti dokumentumot az abban foglalt tartalomnak megfelelően ugyancsak minősíteni kell.

Kiegészítő biztonsági intézkedésnek nem minősülő védelmi eszközök alkalmazására nézve az érdekelt felek megállapodása irányadó.

8. A kiegészítő biztonsági intézkedések, illetve az egyéb külön ráfordításokat igénylő védelmi eszközök alkalmazásának költségei arra hárithatók, akinek érdekkörében az erre vonatkozó igény megjelenik.

Együttes érdekeltség esetén az együttműködő szervek, a rájuk eső rész költségeit viselik, ha az arány nem állapítható meg, a Felek megegyezése, ennek hiányában az egyenlő megosztás elve irányadó.

A végrehajtási utasítás

9. A Rendelet 5. §-ában meghatározottaknak megfelelően, a felügyeletet ellátó miniszterek a Rendelet hatályba lépését követően folyamatosan, de legkésőbb 1981. december 31-ig adják ki utasításaikat a felügyeletük alá tartozó szerveknél érvényes végrehajtási előírásokra.

10. A Rendelet vonatkozó részeiben rögzített tartalmi követelmények mellett különösen az alábbi szempontokat kell figyelembe venni:

— Más, jogszabályokban rögzített előírásokat csak ott és annyiban kell megismételni, illetve értelmezni, amennyiben a szakterület sajátosságai, vagy a számítástechnikai környezetre való alkalmazás azt megkövetelik.

Az alapbiztonság körében elsősorban a technikai, technológiai bizonylati fegyelem betartására, a dokumentációk meglétére, az egységesítési, szabványosítási előírásokra, és egyéb, a fegyelmezett és hatékony működést biztosító feltételekre vonatkozó elveket és szakmai elvárásokat célszerű rögzíteni.

— Átfogó feltételrendszer meghatározásával, szükség esetén részleges, vagy tételes kijelöléssel kell elősegíteni a Rendelet személyi és tárgyi hatályának az érintett szervek által történő egységes értelmezését.

— A kiegészítő biztonsági intézkedésekre, a különleges tűz- vagy vagyonvédelmi feladatokra, a különleges biztonsági, jelző- és riasztóberendezések alkalmazására vonatkozó rendelkezéseket — a fokozatoknak megfelelően (Irányelvek 24—26. pont) — csak a titkot képező adatokkal folyamatosan, illetve előrelátható ismétlődő rendszerességgel munkát végző szervekre nézve kell kötelezővé tenni. A Rendelet 17. § (3) bek. és a 19. § (2) bek. szerinti kijelöléseket egyedileg, az érdekelteknek közvetlenül szóló leirati formában kell kiadni.

Ha az ezen előírások hatálya alá nem tartozó szerveknél eseti igény merül fel ilyen folyamatok ellátására, azt államtitok esetén a felhasználó szerv vezetője, szolgálati titok esetében pedig annak illetékes minősítője egyedi, írásbeli engedélye alapján lehet meghatározott időre folytatni. Az engedély megadásakor a titkot képező adatok kezelésére, feldolgozására, felhasználására érvényes követelmények átmeneti biztosításának, esetleg felváltó (kisegítő) intézkedések megtételének lehetőségét részletesen kell vizsgálni, és a feldolgozás feltételeit meg kell határozni.

A kijelölésekben a fokozott védelmi-biztonsági elvárások körét, illetve a vonatkozó kiegészítő biztonsági intézkedések típusait meg kell határozni, tekintettel arra, hogy a Rendelet 17. § (3) bek. és a 19. § (2) bek. szerinti kijelölést eredményező feltételek eltérő kategóriájúak.

A nagyértékű, nagyteljesítményű számítóközpontok esetén elsődlegesek a műszaki, technikai, technológiai, vagyon- és tűzvédelmi előírások. Az emellett vagy ettől függetlenül titkot képező adatokkal minősített módon dolgozó számítóközpontok esetében ezek az előírások kibővülnek az illetéktelen hozzáférést gátló, elsősorban a Rendelet 11., 14., 16., 17. §-aiban foglalt kiegészítő biztonsági intézkedésekkel.

11. A végrehajtási utasításban, vagy a kijelölésben kell azokat a felmentéseket — időtartam megjelölésével — megadni, amelyekre a felügyeletet ellátó minisztert a Rendelet 27. § (2) bek. jogosítja fel.

Ez esetben a figyelmet a kiváltó (kisegítő) megoldások felkutatásának és alkalmazásának fontosságára fel kell hívni.

12. A végrehajtási utasításban célszerű meghatározni azokat a szempontokat, amelyekkel a felügyeleti szerv a számítás-

ÁBTL - 4.2 - 10 - 21/9/1983 /29

technikai beruházási programok tartalmi előírásait az adatvédelmi intézkedések következtében bővíteni kívánja.

13. Amennyiben a 3/1971. (IX. 23.) BM számú rendelet végrehajtásaképpen kiadott, a titkot képező adatok védelmére vonatkozó általános érvényű utasítások vagy más tárcaelőírások a Rendelet előírásai következtében kiegészítést, módosítást, egybefoglalást vagy értelmezési változásokat igényelnek, ezek átvezetésére vonatkozóan célszerű egyidejűleg intézkedni, és ennek tényét a végrehajtási utasításban rögzíteni, az érintett rendelkezések tételes megjelölésével.

14. A végrehajtási utasításokban, a minősítésnek megfelelő formában utalni kell a tárcaszinten államtitoknak vagy szolgálati titoknak minősített iratok (adatok, információk, témák, területek stb.) jegyzékére, figyelembe véve a 14/1971. (IV. 15.) Korm. számú rendelet előírásait is.

15. A számítástechnikai védelmi szabályzathoz (a továbbiakban: SZVSZ) kapcsolódóan rendelkezni kell:

— a kidolgozás határidejéről a lehetőségekhez igazodó ütemezésben, legkésőbb azonban 1982. június 30-ig,

— szükség esetén a felügyelet alá tartozó szervekre vonatkozó, az SZVSZ felépítésére, tartalmára irányadó további elvárásokról, sajátosságokról.

16. Az adatvédelmi felelősi funkcióra vonatkozóan a végrehajtási utasításban meg kell határozni:

— azokat a feltételeket, amelyek fennállása esetén függetlenített adatvédelmi felelős, esetleg biztonsági apparátus kinevezése kötelező, ajánlott vagy megengedett,

— az adatvédelmi felelős munkaköri besorolásaira, anyagi elismerésének lehetőségeire vonatkozó elveket,

— a szerveknél működő adatvédelmi felelős közvetlen szignalizációs jogkörét,

— a felügyeleti hatóságnál adatvédelmi felelősi feladatkörrel megbízott személy vagy egység kijelölését.

A végrehajtási utasítás részeként, vagy azzal egyidőben célszerű rögzíteni a felügyeleti hatósági adatvédelmi-adatbiztonsági feladatokat.

17. A természetes személyekről elrendelni kívánt számítógépes nyilvántartáshoz, feldolgozáshoz szükséges a Rendelet 21. §-ában előírt engedélyezési eljárás kezdeményezésének, jóváhagyásának és lebonyolításának módját a végrehajtási utasításban szabályozni, illetve rögzíteni a már meglevő, a szervek működési körébe tartozó ilyen jogokat.

18. A Rendelet helyi végrehajtására vonatkozóan külön adatszolgáltatást, vagy rendszeres beszámolási kötelezettséget csak indokolt esetben célszerű előírni.

19. Az egységes gyakorlat kialakítása érdekében, a fentiekben megjelölt szempontok figyelembevételével célszerű egyidejűleg (mellékletként) olyan segédletek közzététele, amelyek a konkrét számítástechnikai szakmai védelmi eszközök körére, egyes terminológiák értelmezésére (távadatfeldolgozás stb.), a rendelkezésre álló technológiai lehetőségekre és berendezésekre, mérési módszerekre, valamint a meghatározható műszaki mutatókra nézve segítséget nyújtanak az érintett szerveknek a SZVSZ összeállításához.

A számítástechnikai védelmi szabályzat (SZVSZ)

20. Az SZVSZ-t az üzemeltető szerv [Rendelet 1. § (1) a) pont] vezetője adja ki, az adatvédelmi felelős (a továbbiakban: AF) előterjesztésében, a szakterületek bevonásával.

21. Az SZVSZ funkciója, hogy rögzítse a számítástechnikai adatvédelem-adatbiztonság feltételeit, környezetét, végrehajtásának rendjét az adott szervnél.

Az SZVSZ akkor tölti be funkcióját, ha mellőzi az általánosságokat, a jogszabályok ismétlését, és a szerv napi munkafeladataira, helyi adottságaira, konkrét problémáira összpontosít.

22. Az SZVSZ minősítését annak tartalma szerint kell elbírálni, de célszerű, ha legalább üzemi titoknak minősül.

Ha az SZVSZ-ben minősített adatok kezelésére vonatkozó utalás vagy előírás van, a minősítésnek a fentinél magasabb fokozatúnak kell lennie. Ezeket azonban célszerű mellékletként külön kezelni, és eltérően minősíteni.

ÁBTL - 4.2 - 10 - 21/9/1983 /31

Ha az SZVSZ-ben eltérő minősítésű részek szerepelnek együttesen, és ezek elválasztása fizikailag, logikailag vagy az áttekinthetőség veszélyeztetése nélkül nem oldható meg a legmagasabb szintű minősítést kell irányadónak tekinteni.

23. Az SZVSZ-nek a már működő, meglevő más eljárásokra csak utalnia kell, részletesen szabályoznia ott és akkor célszerű, ahol azt a számítástechnikai sajátosságok indokolják, ha a különböző területekre vonatkozó előírások összehangolását kell megteremteni, vagy ha az SZVSZ-nek más szabályzatok szigorítását kell megvalósítania.

Az SZVSZ-hez tartalmilag kapcsolható fontosabb belső szabályozások köre:

— tűzrendészeti szabályzat,

— OÉSZ helyi előírásai,

— a beruházások rendjét szabályozó előírások,

— a munkavédelmi szabályzat,

— a rendészeti (portai), más vagyonbiztonsági előírások,

— a technikai, technológiai rendek, műszaki normatívák,

— dokumentációs és egyéb szabványok, előírások, ajánlások, módszerek,

— a szerződéskötések rendje,

— a munkavállalási rend (számítástechnikai szerveknél, ahol a vállalhatóság szempontjából a biztonsági feltételek meglétének, vagy hiányának kérdése is döntő),

— más szervek, vagy rendeletek által előírt telepítési, létesítési, környezeti követelményekre vonatkozó előírások (gépgyártók követelményei, környezetvédelem stb.),

— tárolás, raktározás, szállítás rendje,

— TÜK-kezelés szabályai (beleértve a minősítések és visszaminősítések rendjét, és az iratkivitel rendszerét általában a szervnél),

— kiadványozás, sokszorosítás, publikálás, egyéb nyilvánosságra hozatalt eredményező eljárások működési szabályzata,

— iratkezelés, expediálás, postázás, irattározás, selejtezés, megsemmisítés előírásai,

— a meglevő munkaköri leírások, illetve az egyes egységek funkció-meghatározásai,

— a bel- és külföldi kapcsolatok létesítésének rendje, a kapcsolattartás szabályai,

— az ellenőrzés rendje és munkatervei stb.

Az SZVSZ felépítése és fokozatai

24. A Rendelet 22. §-ának alapján alapbiztonsági fokozatban működőknek tekinthetők azok a szervek, amelyek titkot képező adatokkal számítástechnikai munkafolyamatban nem dolgoznak, ilyent nem tárolnak, illetve számítógépes feldolgozás eredményeképpen létrejött minősített adatot nem használnak, valamint a Rendelet 17. § (3) bek. és a 19. § (2) bek. alapján nem kijelölt üzemeltető vagy felhasználó helyek.

E szerveknél az SZVSZ felépítésében — mint alapkövetelményt — legalább az alábbi tényezőket érvényesíteni kell:

— A szerv biztonsági fokozatát indokoló meghatározás (az alapbiztonságot meghaladó feltételek kizárása).

— Az SZVSZ minősítése.

— Az Irányelvek 23. pontjában meghatározott szabályozások közül azok kijelölése — az adatvédelem belső háttérszabályaiként — amelyek a biztonságos, zavartalan számítástechnikai munkafolyamatok megszervezését, az iratok hibátlanságának, megőrzésének kialakítását, a nagyértékű eszközök és adatok megóvását, az együttműködő felek érdekeinek védelmét, az irányítás és ügymenet megbízhatóságát és naprakészségét biztosítják.

— Mindazon intézkedések elrendelése, amelyek a belső szabályozások meglevő hiányosságainak felszámolására, vagy új szabályozások készítésére vonatkoznak.

— A számítástechnikai munkafolyamatok technikai, technológiai rendje körében az elvárt üzemeltetési, programozási, dokumentációs és egyéb előírások körének kijelölése.

— A szervvel munkaviszonyban, vagy munka végzésre irányuló egyéb jogviszonyban álló természetes személyekhez fűződő számítógépes feldolgozási, vagy adathasználati (tárolási) előírások, a Rendelet 21. §-ának alapján.

ÁBTL - 4.2 - 10 - 21/9/1983 /33

— Az adatvédelmi felelős tevékenységi köre, a működése által érintett más egységeknél szükségessé váló hatásköri, illetékességi módosulások. Az adatvédelmi felelős kötelezettségei és jogai.

— Az üzemi titok minősítésére, védelmére vonatkozó eljárás rendje.

— Az adatvédelmi funkció teljesítéséhez, irányításához, ellenőrzéséhez szükséges, speciálisan e területre vonatkozó belső információrendszer kialakítása.

— A számítástechnika-alkalmazás folyamatában felmerülő külső kapcsolatok létesítésére, fenntartására, beszámolási-ellenőrzési rendjére vonatkozó külön szabályok, amennyiben a szakmai jelleg az általános előírásokhoz képest külön kiterjesztést tesz szükségessé.

— Az SZVSZ kezelésének, terjesztésének, naprakészen tartásának, nyilvántartásának, módosításának, a módosítások átvezetésének rendje.

— Az SZVSZ belső oktatásának, az ismeretek rendszeres bővítésének megszervezése, rendje.

— Az SZVSZ által érintett, annak tartalmát meghatározó jogszabályok tételes felsorolása.

25. A fokozott biztonság kategóriájába sorolhatók azok a szervek, amelyek titkot képező adatokkal — számítástechnikai folyamat közbeiktatásával — munkát végeznek, de nem tartoznak a Rendelet 17. § (3) bek. és a 19. § (2) bek. hatálya alá.

E szerveknél az SZVSZ felépítésére vonatkozó alapkövetelmények az alábbi tényezőkkel bővülnek:

— A számítástechnikai vonatkozású minősítések és visszaminősítések rendje, a minősítésre kijelölt személyek. A minősítési eljárás kezdeményezésének és dokumentálásának ügymenete. A minősítésre vonatkozó felülvizsgálat kötelező gyakorisága.

— Mindazon eseményekre és helyzetekre vonatkozó intézkedések, amelyek a rendeltetésszerű, átlagos napi munkamenet körén kívül esnek, és amelyek bekövetkezésével a szervnél — reális kockázat-elemzés alapján — számolni kell, ideértve olyan eseti, egyedi igények felmerülését, amelyeknek végrehajtása már az alapbiztonsági fokozatot meghaladó működési feltételeket eredményezne.

— A betekintésre (hozzáférésre) jogosultak köre, jogosultságuk terjedelme, az ehhez rendelt biztosító eszközök meghatározása.

A titkos ügykezelés szabályainak a Rendelet szerint számítástechnikai vonatkozású kiterjesztése a 3/1971. (IX. 23.) BM számú rendelet mellékleteként kiadott Szabályzat előírásainak értelemszerű alkalmazásával, valamint a Rendeletben foglaltak figyelembevételével. Az általános fogalmak szakmai értelmezésével, speciális igények megjelölésével, folyamatos üzem esetén készenléti szolgálat megszervezésével.

— Mindazon szakmai (Rendelet 11. §) és biztonságtechnikai (rejtjelzési eszközök, módszerek) adatvédelmi eszközök tételes kijelölése, amelyeket az adott biztonsági fokozathoz igazodóan megállapított veszélyforrásokhoz a szerv vezetője szükségesnek és elégségesnek ítél hozzárendelni.

— A jelzőkészülékek, a távadatfeldolgozás biztonságát szolgáló technikai-műszaki eszközök és intézkedések, valamint más, az adatvédelmi eszközök körében használatos berendezések és eszközök tételes kijelölése, hozzárendelve az azok rendszerbe állítására, folyamatos üzemének megszervezésére, hibátlanságuknak biztosítására, illetve ellenőrzésére vonatkozó előírásokat.

— A szervnél az SZVSZ kiadásakor már meglevő, minősített adatok (témák, területek stb.) jegyzékére történő utalás.

A fokozott biztonság kategóriáján belül eltérést jelentenek azok a szervek, amelyek titkot képező adatokkal munkát nem végeznek, elvileg alapbiztonsági szinten működnek, gyakorlatilag azonban a védelem minősítettebb szintjét követelik meg azok a biztosági igények, amelyeknek teljesítését

— a felügyeleti hatóság elrendelte,

— a szerv vezetője elrendelte, tekintettel a számítóközpont vagy felhasználóhely helyi adottságaira, érdekeire,

— a szerv szerződés vagy más megállapodás formájában elvállalta, együttműködő fél részére.

E szerveknél az SZVSZ felépítésére vonatkozóan a 24. pontban foglaltak irányadók, a követelmények kizárólag a ténylegesen elrendelt vagy igényelt tényezőkkel bővülnek ki.

26. Kiemelt biztonsági fokozatúnak minősülnek mindazon szervek, amelyeket a felügyeletet ellátó miniszter a Rendelet 17. § (3) bek. és 19. § (2) bek. alkalmazásával ilyennek kijelöl.

A kiemelt biztonsági fokozatnál alapkövetelmény, hogy a biztonsági intézkedések szervesen beépüljenek, és rendszerként funkcionáljanak a teljes működés körében, valamint hogy ezek érvényesülését a legszigorúbb ellenőrzésekkel folyamatosan vizsgálják.

Az SZVSZ-nek a szerveknél a 24. és 25. pontban foglaltak maradéktalan érvényesítése mellett ki kell bővülnie

— mindazon kiegészítő biztonsági intézkedések tételes felsorolásával, amelyeknek alkalmazását az Irányelvek 1. pontjában felsorolt források bármelyike rögzít, a felügyeleti kijelölés előír, illetve a szerv vezetője elrendel,

— a rendkívüli események bekövetkezésére előírt intézkedési tervek számítástechnikai vonatkozású kiterjesztésével,

— a biztonságtechnikai eszközök alkalmazásához szükséges bejelentési, egyeztetési és engedélyeztetési eljárások meghatározásával.

Az adatvédelmi felelős (AF)

27. A biztonsági feltételek elrendeléséért és megvalósításáért a szerv vezetője felelős. Az AF alapvető funkciója, hogy a Rendeletben, az Irányelvekben, a végrehajtási utasításokban és az SZVSZ-ben rögzített feladatait teljesítve a szerv adatvédelmi-adatbiztonsági szempontokat kielégítő működését a ráruházott hatáskör keretében biztosítja.

Az AF feladatai nem érintik a szerv munkatársainak személyes felelősségét a végrehajtás tekintetében.

28. Az AF munkakörének meghatározásához a helyi sajátosságok érvényesítése mellett az alábbi fontosabb elveket, illetve szempontokat célszerű követni, a védelmi fokozatnak megfelelő feladat-kijelölésekkel:

Az AF kötelezettségeire vonatkozó ajánlások:

— Az SZVSZ kidolgozása, naprakészen tartása.

— A minősítők körére, a betekintési (hozzáférési) jogosultságra vonatkozó javaslattétel, döntéselőkészítés, a jegyzékek naprakészen tartásának ellenőrzése.

— Új védelmi eszközök szükségessége, vagy egyedi esetekre alkalmazandó védelmi eszközök igénye esetén az elrendelés kezdeményezése.

— A veszélyforrások körében bekövetkező változások folyamatos vizsgálata, követése.

— A védelmi eszközök alkalmazására vonatkozó komplex döntéselőkészítés érdekében a kockázati tényezők és a ráfordítások folyamatos elemzése a megfelelő szakterületek bevonásával, a biztonsági színvonal elérését kielégítő intézkedések kialakítása.

— Az adatvédelem-adatbiztonság témakörében külső szervekkel kapcsolatok tartása. Engedélyezési, jóváhagyási eljárások kezdeményezése, a szükséges előterjesztések összeállítása.

— Jelzőkészülékek, műszeres bemérések stb. meglétének és szabályszerű üzemeltetésének, folyamatos szerviz-ellátottságának ellenőrzése.

— A TÜK-előírások felügyelete, decentralizált (szakmai) TÜK esetén annak irányítása, vagy biztonsági szakfelügyelete.

— Külföldi iratkivitel engedélyezésének előkészítése; számítástechnikai adathordozók esetén az irat technikai ellenőrzése, illetve ellenőrzésének megszervezése.

— Egyes selejtezési-megsemmisítési eljárások ellenőrzése.

— Az adatvédelmi tevékenység megszervezését és ellenőrizhetőségét támogató nyilvántartási rendszer kialakítása.

— Főtevékenységként számítástechnikai szolgáltatást nyújtó szerveknél a felhasználók szakmai segítése adatbiztonsági kérdésekben.

— A szerv szervezeti és működési szabályzata érintett részeinek biztonsági szempontból történő véleményezése.

— Munkavállalások, külső kapacitás igénybevétele és más szerződéskötések során a biztonsági követelmények érvényesítése, illetve a végrehajtás feltételrendszerének véleményezése.

— A szerv egységeiben folyó adatvédelmi tevékenységek koordinálása.

— az adatvédelmi-adatbiztonsági feladatok folyamatos belső ismertetése, oktatása.

— A hatáskörébe tartozó területeken folyamatos és tervszerű ellenőrzés.

Az AF jogait úgy kell meghatározni, hogy azok a kötelezettségei teljesítéséhez szükséges hatáskört és feltételeket megfelelő mértékben és módon biztosítsák.

NYITRAI FERENCNÉ dr. s. k.,
elnök