Tóth András
toth.hir.andras@zmne.hu

A ZÁSZLÓALJ INFORMATIKAI RENDSZEREI ALKALMAZÁSÁNAK SZABÁLYAI, AZ INFORMATIKAI TEVÉKENYSÉGEK VÉDELMI FELADATAI

Absztrakt

A zászlóalj informatikai rendszere az alegység állapotára, helyzetére és feladataira vonatkozó, ezzel összefüggő hírek, értesülések, adatok megszerzése, továbbítása, átalakítása (feldolgozása), tárolása, visszakeresése, valamint rendelkezésre bocsátása érdekében végrehajtott tevékenységek összességét hívatott kiszolgálni. A rendszer zavartalan üzemelése szempontjából az informatikai szakállomány minden felhasználó számára kötelező érvényű rendszabályokat dolgoz ki, amelyek maradéktalan betartása mellett csökkenthető, elkerülhető az eszközök, valamint a hálózat meghibásodása.

The IT system of the battalion is able to serve the purchase, the forwarding, the converting and the storage of the news, the information, and the data of the sub-unit's status, position and functions. The IT staff develops regulations to the smooth functioning of the system, which would be adherence for all users to reduce, to avoid the failure of the equipment and net.

Kulcsszavak: *vírusvédelem, illetéktelen hozzáférés, elektronikus információvédelem, titokvédelem ~ virus protection, unauthorized access, electronic information security, privacy*

A SZAKINFORMATIKAI TEVÉKENYSÉG

A szakinformatikai tevékenység speciális szakmai előképzettséget, felkészültséget igényel, és általában e célra külön rendszeresített személyek, vagy szervezeti elemek végzik (vagy végezhetik). A tevékenység körébe tartoznak: az információrendszer szervezése, a rendszerelemzés, a programozás, az informatikai szakanyag és szoftver beszerzése, a technikai karbantartás, a szervízszolgáltatás, a műszaki fejlesztés, a szakellenőrzés, az adatvédelmi és vírusvédelmi eszközök telepítése.

A zászlóalj szakinformatikai szervezet jogát és kötelességeit a dandár G-6[1] főnökség informatikai tisztje és informatikai beosztottja, valamint a zászlóalj informatikai beosztású katonái együttesen gyakorolják.

AZ ÁLTALÁNOS INFORMATIKAI TEVÉKENYSÉG

Az információfeldolgozás körébe vont adatok összegyűjtését, továbbítását, felhasználását, tárolását, visszakeresését és rendelkezésre bocsátását, valamint az egyéb a szakinformatikai, tevékenységek körébe nem sorolható tevékenységeket általános informatikai tevékenységnek nevezzük. Az általános informatikai tevékenységeket a felhasználók és adatszolgáltatók speciális előképzettség nélkül, a szükséges mértékű betanítás, kiképzés után önállóan végezhetik. Szükség esetén a szakinformatikai állománytól kérhetnek szakmai támogatást.

1 Híradó és Informatikai Részleg

Az informatikai védelem

Az adatok védelmére csak az elöljárói intézkedések által engedélyezett, és a központi nyilvántartásban szereplő védelmi eljárásokat szabad alkalmazni.

Az illetéktelen hozzáférés elleni védelem

Adatvédelmi szempontból minősített és nyílt munkahelyeket különböztetünk meg. A katonai szervezet vezetője jelöli ki a minősített adatok tárolására szánt munkahelyet, amelyet be kell bejelenteni a G-6 főnökségség informatikai tisztjénél. Minősített információt csak a bejelentett számítógépen szabad feldolgozni. Az olyan számítástechnikai berendezések részére, amelynek beépített, vagy háttér adattárolója minősített adatot tartalmaz, a munkavégzés ideje alatt folyamatos felügyeletet, azon túl pedig az ügyviteli szerv helyiségének védelmére meghatározott feltételeket kell biztosítani.

Minősített adatokat tartalmazó, fix merevlemezes, mágneses adathordozót meghibásodása esetén polgári vállalatnak javítás céljából átadni tilos. Ezek javítására, megsemmisítésére a vonatkozó, érvényben lévő előírásoknak megfelelően a kijelölt szakinformatikai szerv (területi szerviz, szakszolgálat) intézkedik. A minősített adatokat tartalmazó eszközök javítását polgári vállalat kizárólag a helyszínen, az illetékes szakszolgálat szakmai felügyelete mellett végezheti.[2]

A kihelyezett terminálok és munkaállomások képernyői a rajtuk megjelenített adatokkal azonos minősítésű iratnak tekintendők. Azok aktuális minősítésének felismerhető jelöléséért, valamint annak megfelelő titokvédelméért annak az osztálynak (alosztálynak) vezetője felel, akinél a berendezés üzemel.

Az alkalmazott hozzáférés elleni védelmi eljárásoknak biztosítani kell az informatikai rendszerbe történő illetéktelen behatolási kísérletek megakadályozását és ezek dokumentálását, a hozzáférés-, program- és adatvédelem megvalósítását. A hozzáférés elleni védelemnek biztosítani kell a felhasználók azonosítását, a hozzáférési igény jogosultságának ellenőrzését, a jogosultságnak megfelelő erőforrások igénybevételét, valamint a felhasználónak nyújtott szolgáltatások feljegyzését, naplózását. A programvédelem biztosítja, hogy a felhasználó csak azokat a programokat, utasításokat hajthassa végre, amelyeket a rendszer működtetéséért (felügyeletéért) felelős személy (supervisor, adatbázis adminisztrátor) a számára engedélyezett, és egyben megakadályozza a nem engedélyezett utasítás (például: programmásolás, módosítás, felülírás, törlés) végrehajtását.

Az Internetre ideiglenesen vagy állandó jelleggel rákapcsolt számítógépeken, a Magyar Honvédséggel kapcsolatos adat tárolása és feldolgozása tilos. Tilos az Internetre az olyan számítógép rákapcsolása, amely lokális hálózat tagjaként üzemel. Az Internet igénybevételére csak fizikailag elkülönített számítógépet lehet használni. Minősített, nyílt illetve belső használatra nyilvános adatok Interneten történő továbbítása szintén tilos.[3]

Rejtjelzéssel történő védelem

Az adatok továbbításánál, a védelem hatékonysága érdekében mindig olyan rejtjelző (kódoló) eszközt és eljárást kell alkalmazni, melynek a biztonsági hatékonysága arányban áll a közlemény fontosságával, minősítésével. A katonai szervezetek informatikai rendszereiben a továbbításra kerülő minősített információk védelméhez csak a rendszeresített, a központilag kiadott, illetve az arra jogosult rejtjelző szervek által kidolgozott rejtjelző eszközöket, programokat és kulcs dokumentációkat szabad használni, az eszközökhöz külön-

2 ÁLT/3 HM és MH Titokvédelmi és Ügyviteli Szabályzata

3 A Magyar Honvédség parancsnokának, vezérkari főnökének 81/1997. (HK 20.) intézkedése az Internet igénybevételével kapcsolatos titokvédelmi és adatbiztonsági rendszabályok betartásáról

külön meghatározott módon. A dandár informatikai rendszerében alkalmazott rejtjelzéssel történő védelmi eljárások bevezetésére, a védelmi eljárásba vonható személyek kijelölésére a dandár parancsnoka külön intézkedik. Rejtjelző eszköz az Internethez nem csatlakoztatható.[4]

Számítástechnikai titokvédelem (adatvédelem, adatbiztonság)

Az adatvédelem célja, hogy az informatikai rendszer adatait csak az módosíthassa, törölhesse, aki az adatokért felelős. A számítástechnikai titokvédelmi felügyelettel összefüggő feladatok elvégzésére a dandár G-6 főnökség információvédelmi tiszt van kijelölve.

A minősített adat adathordozón történő tárolása és továbbítása, vagy szállítása esetén az adathordozó jellegének megfelelő (fizikai mechanikai, hő, vegyi) védelmet kell biztosítani, a mágneses adathordozót óvni kell a közvetlen elektromágneses behatástól.

Az adatállományok megőrzéséért és rendszeres mentéséért, illetve visszatöltéséért az adatállomány létrehozásáért és karbantartásáért az adatgazda felel. Az adatállományok archiválása mindig dokumentációban előírtak alapján történik, programrendszerek megőrzéséhez hasonlóan.

Minősített adatállományok, valamint pótolhatatlan adatok tárolása két-két lehetőleg független adathordozón, egyik példánya számítógépnél, a másik példánya másodlagos adattárban történik. A másodlagos adattárban elhelyezett adatállományok aktualizálásáról, ellenőrzéséről az adatot szolgáltató köteles gondoskodni.

Biztosítani kell, hogy az informatikai rendszerbe csak az arra illetékes személyek léphessenek be. Lehetőleg hardveres és szoftveres úton is biztosítani kell a belépési jogosultságok ellenőrzését, a jogosulatlan belépés kizárását.

Amennyiben a számítástechnikai eszköz felhasználási területe megváltozik, a rajta található minősített adatokat archiválni és az adattárolót formattálással törölni kell.

A számítógépes vírusok elleni védelem

Előre nem látható rendkívüli események (rendszerkatasztrófa, elemi csapás, tűzeset, stb.) esetére az informatikai rendszerek működésének helyreállítására katasztrófatervet kell készíteni. A terv tartalmazza a helyreállítandó rendszerkomponensek kijelölését, a rendszerszoftverek, alkalmazói programok, adatállományok felsorolását, a tartalék (háttér) számítógép kijelölését, a másodlagos adattár helyét, a helyreállítás menetének ütemtervét és a helyreállításra kijelölt személyeket.

Minden olyan munkahelyen, ahol számítógépes hálózat működik, úgynevezett "vírusvédelmi beléptetési pontot" kell létrehozni. A "vírusvédelmi beléptetési pont" egy önálló berendezés, amelyen a programok telepítése előtt minden új programot és adathordozót ellenőrizni, illetve futtatni kell. Másik berendezésben csak az itt hibátlannak talált program illetve adathordozó használható fel.

Az adatvédelmi és adatbiztonsági rendszabályokban meghatározott időközönként, illetve szükség szerint teljes körű (az ismert vírusokra kiterjedő) vírusellenőrzést kell végezni a rendszeresített védelmi szoftverekkel. Az híradó és informatikai részleg negyedévente végez központilag irányított vírusvédelmi ellenőrzést.

A zászlóaljnál a központilag biztosított vírusvédelmi eszközök telepítését a 43. Nagysándor József Híradó és Vezetéstámogató Ezred, Híradó és Informatikai Központ állománya végzi. A zászlóalj informatikai hálózatában csak a Magyar Honvédség által biztosított szoftverek adathordozók használhatók.

Az alkalmazók szakmai felkészítésekor ki kell térni a vírusok elleni védelem rendszabályainak ismertetésére, valamint a védelmi eszközök használatára.

4 43/1994. (HK 09.) kormányrendelet a rejtjeltevékenységről

A vírusfertőzés észleléskor az alábbi intézkedéseket kell tenni:

a. Fertőzött rendszerek izolálása, elkülönítése (az eszköz kikapcsolása, az ott használt adathordozók elkülönítése, használatból kivonása);
b. Az észlelt jelenség feljegyzése;
c. Az illetékes informatikai szakállomány értesítése;
d. Annak kiderítése, hogy honnan és hogyan jutott be a vírus, ha ez lehetséges;
e. A fertőzés azonosítása és a fertőzés megszüntetése;
f. A vírusfertőzéskor és utána megtett ellenintézkedések regisztrálása.

A tűzvédelem

Azok a helyiségek, melyekben informatikai berendezéseket üzemeltetnek eltérő rendelkezés hiánya esetén a "D" tűzveszélyességi osztályba tartoznak. A zászlóalj Tűzvédelmi Tervébe a létesítményeket e sajátosságok alapján kell besorolni, és a vonatkozó rendszabályokat meghatározni.

Az üzemeltető szervezetek vezetői kötelesek gondoskodni arról, hogy a területükön létesített és üzemeltetett berendezések működtetése az előírások szerint történjen.

Az elektromos berendezéseket a munkaidő végeztével áramtalanítani kell. Az üzemeltetési helyen legfeljebb egynapi üzemeltetéshez szükséges papírból készült adathordozó tárolható, valamint tilos a helyiségben tűzveszélyes folyadékot tárolni. A villamos berendezéseket és a villámhárítót háromévenként tűzvédelmi szempontból felül kell vizsgálni. Minden olyan helyiséget, amelyben központi számítógéprendszer, vagy hálózati szerver üzemel halon oltóval kell felszerelni. A többi helyiségeket (szükség szerint) tűzoltó készülékkel kell ellátni. Az alkalmazókat tűzvédelmi oktatásban kell részesíteni. Ki kell jelölni, és szabadon kell tartani a menekülési útvonalakat, valamint a vészkijáratot.

Egyéb védelem

Az egyéb védelem feladata az előző védelmi kategóriákba nem sorolható veszélyforrások elleni védelmi rendszabályok meghatározása. A munkavédelem, az érintésvédelem, balesetvédelem, a vagyonvédelem, az elektronikai felderítés és zavarvédettség vonatkozó rendszabályainak rögzítése.

Az informatikai eszközök alkalmazásakor lehetőség szerint gondoskodni kell az alkalmazói állomány munkavégzéssel összefüggő ártalmainak csökkentéséről. A megfelelően kialakított és elhelyezett bútorzattal, a megvilágítási viszonyok kedvező kialakításával, sugárzás csökkentő eszközök – monitorszűrő, védőszemüveg – alkalmazásával.

Az informatikai eszközöket tartalmazó helyiségeket megfelelő védelmi eszközökkel – ráccsal, biztonsági zárral, pecséttel – kell ellátni, lehetőség szerint tűz és vagyonvédelmi jelzőberendezéssel kell felszerelni, illetve ezeket a rendszereket üzemben kell tartani.

Fel kell mérni az elektromos zavarforrásokat, el kell hárítani, illetve csökkenteni kell hatásukat. A hibás berendezéseket (zavarforrásokat) meg kell javíttatni, megfelelő árnyékolást kell alkalmazni, illetve át kell telepíteni megfelelőbb helyre. Az elektromágneses sugárzás elleni védelem érdekében a mágneses adathordozókat megfelelően árnyékot tároló helyen (csomagolásban) kell tárolni és szállítani.

FELHASZNÁLT IRODALOM

- 166/1990. (HK 23.) MH HVK Hír. és Aut.Csf. együttes intézkedése az információvédelem anyagi-technikai biztosításának megszervezéséről és a közös feladatok végrehajtásáról
- 104/1992. (HK 23.) MH HVK HIRICSF intézkedése a számítógépes rendszer- és alkalmazói programok anyagnemfelelősi teendőinek szabályozásáról
- 11/1995. HM rendelet a katonai vonatkozású állami- és szolgálati titok köréről
- 43/1994. (HK 09.) kormányrendelet a rejtjeltevékenységről
- A Magyar Honvédség parancsnokának, vezérkari főnökének 81/1997. (HK 20.) intézkedése az Internet igénybevételével kapcsolatos titokvédelmi és adatbiztonsági rendszabályok betartásáról
- ÁLT/3 HM és MH Titokvédelmi és Ügyviteli Szabályzata
- ÁLT/210 MH Informatikai Szabályzata
- 179/2003 (XI.5.) Kormányrendelet
- 180/2003 (XI.5.) Kormányrendelet
- 1995. évi LXV. Törvény az államtitokról és a szolgálati titokról