AZ INFORMÁCIÓ VÉDELME AZ AUTOMATIZÁLT INFORMÁCIÓS RENDSZEREKBEN

AJLAMAZJAN, A. K. – DENISZENKO, A. V.: Zascsita informacii v ÉVM c. írása alapján (Problemü MSZNTI, 1980. 1.no. 66–94.p.) HOPPÁN GÉZA tömörítvénye.

Az információ védelme kifejezés többféleképpen értelmezhető. Jelenti egyrészt az információnak és hordozójának (dokumentum, gépi adathordozó stb.) megóvását a fizikai (nem emberi beavatkozás jellegű) károsodástól vagy megsemmisüléstől. Ebben az összefüggésben a védelem tárolástechnikai probléma. A másik lehetséges értelmezése (és a továbbiakban csak ilyen összefüggésben szerepel): az információ védelme az illetéktelen hozzáféréssel, felhasználással és megváltoztatással szemben. Ez utóbbi szempont különösen a gépi adathordozók esetében fontos követelmény, ahol az információ az ember számára közvetlenül érzékelhetetlen formában tárolt, könnyen és gyorsan megváltoztatható anélkül, hogy ennek bármilyen észrevehető jele lenne, autentikus volta nem, vagy csak igen nehezen ellenőrizhető.

Védelemre nemcsak az úgynevezett bizalmas jellegű információ esetében van szükség. Az információ mindinkább közvetlen termelőeszközzé válik. Gyűjtése, előállítása és szolgáltatása munkával és költségekkel jár. Így, minden más áruhoz hasonlóan meghatározott árat kell fizetnie annak, aki birtokába kíván jutni.

A számítógépes információs rendszerek és adatbankok kialakulásának és működésének kezdeti szakaszában az információ védelme nem okozott különösebb gondot. A felhasználó (megrendelő vagy előfizető) sem az adatbázissal, sem a számítógéppel nem került közvetlen kapcsolatba. Kérdését, igényét eljuttatta a teljesítőhöz (a rendszer üzemeltetőjéhez), és a teljesítő gondoskodott a kérdés feldolgozásáról, a válasz kiadásáról.

A hatvanas évek második felétől kezdett a helyzet megváltozni. Egyre nagyobb teljesítményű számítógépek jelentek meg, melyek kapacitását egyetlen adatbank kiszolgálása már nem tudta teljes mértékben lekötni, ezért az ilyen nagyteljesítményű számítógépekre több, különböző adatbázist szerveztek. Ez már önmagában is szükségessé tette az egyes bázisok elkülönített kezelését.

A másik lényeges változást az úgynevezett on-line hálózatok kialakulása jelentette. Ezekben a rendszerekben a felhasználó (előfizető) saját terminájáról valamilyen távközlési vonal közbeiktatásával közvetlen kapcsolatot teremt a fizikailag akár többszáz kilo-

méter távolságra lévő számítógéppel és azon keresztül az adatbázissal. A terminál használója közvetlenül képes utasításokat adni a számítógépnek, ezáltal részben átveszi a számítógép operátorának funkcióját. Utasításait megfelelő kódszavak formájában közli a számítógéppel. Ezek a kódszavak aktivizálnak bizonyos, a számítógépben tárolt, úgynevezett alkalmazói programokat, illetve kijelölik azt az adatbázist, vagy annak megfelelő részét, mellyel a meghívott programnak dolgoznia kell. A számítógép munkájának eredményét (outputját) közvetlenül kiadja a terminál képernyőjére és/vagy kiíróberendezésére.

Az ilyen típusú hálózatok gyors terjedését mindenekelőtt az magyarázza, hogy jelentősen meggyorsítják az előfizető és a számítógép üzenetváltását. Az on-line hálózatok kialakulását megelőzően a felhasználó kérdésének eljuttatása a feldolgozás helyére (a számítógép telephelyére), valamint a számítógép válaszának megküldése a felhasználó részére hagyományos módon (postán, küldönccel stb.) történt, és ez olykor igen lassúnak bizonyult. Bár a számítógépes feldolgozás önmagában csak néhány negyedórát vett igénybe, a felhasználó – számítógép – felhasználó üzenetváltáshoz olykor egy teljes hétre is szükség volt. Az on-line kapcsolat kialakításával viszont az üzenetváltás az elektronikus jelátvitel sebességére gyorsult fel, ezzel gyakorlatilag lehetségessé vált a párbeszéd.

Mivel a felhasználó termináljáról közvetlenül hozzáférhet a központi számítógéphez és ezen keresztül az adatbázishoz, ezt a hozzáférést az információ védelme érdekében valamilyen módon szabályozni kell, esetleg differenciált szabályozásra is szükség lehet, amennyiben a rendszer – üzleti vagy egyéb megfontolásból – különbséget tesz a felhasználók között hozzáférési jogaikat illetően.

Egyes esetekben egy központi számítógépen keresztül több, különböző adatbázis érhető el. Ilyen például az EURONET rendszer, vagy az IAEA bécsi központjának számítógépe, mely az INIS és AGRIS adatbázisokhoz biztosít hozzáférést. Az INIS adatbázis tekintetében az AGRIS előfizetője illetéktelen használónak minősül és ugyanez a helyzet megfordítva is. Külön védelemben kell tehát részesíteni az egyes adatbázisokat.

Előfordulhat, hogy egyetlen adatbankon belül is szükség lehet bizonyos adatcsoportok megkülönböztetett kezelésére. Ilyen helyzet áll elő például akkor, ha az adatbázis faktográfiai adatokat is képes szolgáltatni, de ezt külön díj ellenében teszi, vagy egy személyi nyilvántartás egyébként nyílt jellegű adatai között bizalmas kezelést igénylő (például orvosi titoktartás alá eső) adatok is szerepelnek. Természetesen a megkülönböztetetten kezelt adatokat differenciált védelemben kell részesíteni, és a felhasználók között is különbséget kell tenni aszerint, hogy hozzáférési joguk milyen adatokra vonatkozik.

Olykor az alkalmazói programok hozzáférhetőségét is differenciálni kell. Indokolt lehet például egy statisztikai kigyűjtést végző alkalmazói program hozzáférhetőségének korlátozása.

A hozzáférés tekintetében differenciált adatcsoportok kialakítása egy további előnnyel is jár. Mivel a program csak a felhasználó számára hozzáférhető adat-frakcióval dolgozik, csökkenni fog a feldolgozásra fordított gépidő.

Az elmondottak alapján az automatizált számítógépes információs rendszerekben a védelem alapvető feladata a következő: a rendszernek meg kell állapítania, hogy a terminálon keresztül kivel áll kapcsolatban (azonosítania kell a felhasználó személyét), majd

az azonosított felhasználó számára biztosítania kell a megfelelő hozzáférési jogokat, ugyanakkor meg kell tagadnia tőle mindazt, amire nem jogosult.

Az automatizált információs rendszerekben e feladat ellátására különböző eszközöket és módszereket alkalmaznak. Az eszközök első csoportját az *adminisztratív eszközök* alkotják. Olcsó és egyszerű megoldást jelentenek, ám önmagukban nem mindig tökéletesen megbízhatók. Tulajdonképpen rendszeren kívüli eszközök és azoknak az intézkedéseknek összességét jelentik, melyek a terminál használatát, a kapott információ kezelésének, felhasználásának, tárolásának rendjét, stb. szabályozzák.

A rendszeren belüli védelmi eszközök a rendszer integráns részét alkotják, ezen belül lehetnek műszaki (hardware vagy berendezés jellegű) és programtípusú (software) eszközök. A *műszaki eszközök* alatt maga a számítógép és kiegészítő (periferikus) berendezései értendők, melyeknek az adott védelmi funkció ellátásához meghatározott karakterisztikával kell rendelkezniük. A számítógépnek kellő tárolókapacitással kell rendelkeznie ahhoz, hogy a védelmi funkciókat ellátó programokat, a felhasználók és jogaik, jelszavaik listáit, stb. tárolni legyen képes; a terminálóknak esetenként programozhatóknak kell lenniük, kódoló és dekódoló, személyi kártya azonosító berendezéseket kell tartalmazniuk stb.

A *program típusú eszközök* szerepe a védelemben a felhasználó azonosításánál, majd az azonosítást követően a megfelelő alkalmazói programok és adatcsoportok felszabadításánál, illetve mások felé a hozzáférés lezárásánál van. Felügyelik az alkalmazói programok működését, azokkal szemben elsőbbséget élveznek. Meg kell akadályozniuk az alkalmazói programok működése során azok leolvasását vagy megváltoztatását.

A felhasználó azonosítására többféle módszer alkalmazható. Az úgynevezett *antropometrikus módszerek* a felhasználót biológiai vagy ahhoz közelálló tulajdonságai alapján azonosítják. Ilyenek például a fénykép, az ujj- vagy tenyérlenyomat, a beszédhang, stb. alapján azonosító eljárások. Jóllehet igen megbízhatóak, felismerési pontosságuk megközelíti az emberi felismerését és garantálják a felhasználó jogainak átruházhatatlanságát, komoly hátrányuk, hogy rendkívül költséges, eszközigényes és bonyolult eljárások, ezért alkalmazásuk csak kivételes esetekben indokolt, általános elterjedésük nem várható.

Olcsó módszert jelentenek az *azonosító kártyák.* Ennél a módszernél személyre szóló azonosító kártyákat adnak ki, melyet külön berendezés ellenőriz. A módszer hátránya, hogy nem a felhasználó személyét, hanem a kártyát azonosítja. Rendszeren kívüli eszközökkel kell megoldani, hogy a kártyákat helyesen szolgáltassák ki, azok utánozhatatlanok és átruházhatatlanok legyenek. Komoly zavar származhat abból, ha a kártya elvész vagy megsemmisül.

A felhasználó azonosítására leggyakrabban a *jelszavas vagy listás módszert* alkalmazzák. A felhasználó a megfelelő jelszó közlésével teremthet kapcsolatot a rendszerrel. Az eljárásnak két alapvető típusa van.

Az első esetben a rendszerhez hozzáférést egyetlen közös jelszó engedélyezi valamennyi felhasználó számára. A jelszót a rendszer adminisztrációja szolgáltatja ki az előfizetőnek. A rendszer mindazok számára hozzáférhető, akik az adott jelszó birtokában vannak. Ez az egyszerűbb eljárás. Adminisztratív eszközökkel kell elérni azt, hogy a fel-

használónak ne álljon érdekében a jelszó átruházása. Szükség esetén a hozzáférési jog úgy differenciálható, hogy minden megkülönböztetett módon kezelt adatcsoporthoz vagy alkalmazói programhoz külön jelszót rendelnek hozzá. Ilyen esetben természetesen a felhasználónak egyetlen összeköttetés során is mindannyiszor közölnie kell a megfelelő jelszót, valahányszor újabb, külön jelszóval védett objektumhoz kíván fordulni.

A jelszavas módszer alkalmazásának másik formájánál (a listás módszernél) minden felhasználónak egyedi jelszava van, melynek közlése szabad utat biztosít valamennyi, számára hozzáférhető adatcsoporthoz és programhoz. Ezt a jelszót adhatja a rendszer, de választhatja a felhasználó is. Ilyen esetben minden, a védelem szempontjából megkülönböztetett objektumhoz (adatcsoporthoz, programhoz) hozzá kell rendelni az adott objektum jogosult használóinak (pontosabban azok jelszavainak) jegyzékét (listáját).

A jelszóval szemben támasztott követelmények közé tartozik, hogy az viszonylag könnyen megjegyezhető, ugyanakkor nehezen megfejthető legyen. Ez utóbbi követelménynek tesznek eleget az úgynevezett többlépcsős jelszavak, amikor – a számítógéppel folytatott párbeszéd formájában – több jelszót kell a megfelelő sorrendben közölni ahhoz, hogy a rendszer hozzáférhető legyen.

A megfejtés elleni védelmet szolgálja a jelszó megújításának módszere is. Ennek lényege, hogy a hozzáférést nem egy állandó jelszó közlése adja meg, hanem minden újabb kapcsolat létesítésekor előre megadott jelszóképzési kulcs alapján az előző alkalommal használt jelszót alapul véve új jelszót kell képezni. (Az utoljára használt jelszót maga a számítógép adja ki a terminálra az összeköttetés létrejöttekor.) Jelszóképzési módszer lehet például a következő: a régi jelszó második és harmadik jele közé be kell iktatni az aznapi dátumot, ugyanakkor el kell hagyni a végéről a kiegészítésnek megfelelő számú jelet; vagy a második betűt a betűrendben utána következő betűre kell cserélni. Természetesen a számítógép maga is előállítja az új jelszót és azt összehasonlítja a terminálon közölt jelszóval.

A kevésszámú jelből álló jelszavak programozható terminál segítségével viszonylag rövid idő alatt megfejthetők. Ez ellen úgy védekeznek, hogy a számítógép néhány sikertelen jelszóközlési kísérlet után automatikusan lekapcsolja a terminált és a sikertelen kísérletről feljegyzést készít.

A felhasználó azonosítása és ezzel az egész védelmi rendszer értelmét veszítheti, ha a kapcsolat létrejöttekor vagy annak folyamán a védelem a távközlési vonalban meghibásodik. A távközlési vonalban adódó hibák okozhatják azt, hogy a helyesen közölt jelszót a rendszer hibásnak értékeli, a rendszer hibás terminál-címre adja ki a feldolgozás eredményét, vagy a megszakadt távközlési vonal helyreállításakor helytelen összeköttetés jön létre. Ilyen hibák nem ritkák az átkapcsolásos rendszerű távközlési vonalaknál.

A védekezés legáltalánosabb módja, hogy bármilyen zavar esetén – a sikertelen jelszóközlési kísérletekhez hasonlóan – a számítógép automatikusan lekapcsol a terminálról és a zavar elhárítása után elölről kell kezdeni a kapcsolat felvételét. Tökéletesebb és többirányú védelmet biztosít a kódolás. Ilyenkor a jelszó közlésétől kezdve a teljes párbeszéd kódolt formában bonyolódik. Ennek természetesen adott műszaki feltételei (kódolásra és dekódolásra alkalmas központi számítógép és terminál) vannak. Ilyen esetben csak a hívó terminálon „értelmes" a válasz, az esetleges téves címre csak

értelmetlen jel-kombináció érkezik, mivel a kódolási-dekódolási rendszer terminál-specifikus.

Az eddig elmondottak csak az úgynevezett statikus, tehát a rendszerben változatlan formában jelenlévő információ vonatkozásában hatékonyak. Az eredeti adatállományban nem szereplő, a feldolgozás folyamán keletkezett új, úgynevezett dinamikus információ (összesített adatok, átlagok, trendek, statisztika, különböző mutatók stb.) védelme egyenlőre megoldatlan kérdés.

Újabban vannak kialakulóban az interaktív rendszerek. Itt a felhasználó a rendszer kínálta adatokon és programokon kívül saját adataival és programjaival is dolgozhat, sőt, a felhasználók egymásnak is átengedhetik saját adataik és programjaik használatának jogát. Ilyenkor meglehetősen bonyolult programozás-technikai eszközökkel és adatvédő cimkék (védő bitek, védő deszkripotorok) alkalmazásával kell biztosítani, hogy az arra jogosult felhasználók mások adatait és programjait használhassák ugyan, de azokat megváltoztatni csak a bevivő legyen képes. Ilyen rendszereknél sem oldották még meg a védelem valamennyi problémáját.

Összefoglalóul elmondható, hogy az információ védelme objektív követelmény minden olyan rendszerben, mely nagy számítógépes komplexumot és adatátviteli hálózatot tartalmaz. A védelem nemcsak az információ esetleges bizalmas jellegének megőrzéséhez szükséges, üzleti megfontolásokon túlmenően a feldolgozás idejét is csökkentheti. A védelem a hagyományos szervezési és adminisztratív eszközökkel megnyugtatóan nem oldható meg. A kellő védelem biztosításához külön műszaki és program-típusú eszközök szükségesek. A felhasználót azonosító és ezáltal a szabályozott, esetenként differenciált hozzáférést lehetővé tevő módszerek, de egyben az egész védelmi rendszer hatékonysága és költsége egyenesen arányos.

Mindeddig nem sikerült „egyedül üdvözítő", azaz bármely automatizált információs rendszer esetében elfogadható költségek mellett maximálisan hatékony védelmet nyújtó védelmi rendszert kialakítani. Általában az egyszerűbb, kevésbé strukturált rendszerek (csak statikus adatokkal dolgozó, a felhasználó kategóriákat kevésbé differenciáló, nem interaktív rendszerek) védelme egyszerűbb és olcsóbb módszerekkel is megfelelően ellátható. A védelmi rendszert mindig az adott információs rendszer céljának, védelmi igényének megfelelően kell kialakítani.

Az automatizált információs rendszerek egyre változatosabb szolgáltatásokat kínálnak. A terminálok alkalmazása a legkülönbözőbb szférákban (ügyvitel, oktatás, orvosi ellátás, jogtudomány, stb.) terjed, a technika fejlődése (műholdas távközlés, számítógépek, terminálok műszaki fejlesztése) ezt a folyamatot gyorsítja és mind általánosabbá teszi. Optimista becslések a terminálok várható elterjedését egyenesen a telefonéval vetik össze. Ezért a jövőben az információ védelmének várhatóan egyre nagyobb és összetettebb feladatokkal kell megbirkóznia, ez azonban ugyanakkor gyors fejlődést és új, esetleg meglepő eredményeket enged sejtetni ezen a területen.