Mr. Željko Hutinski

Fakultet organizacije i informatike
V a r a ž d i n

UDK: 007.5
Stručni rad

PRISTUP KLASIFIKACIJI UGROŽAVANJA IFORMACIJSKIH SISTEMA

U radu se prikazuje nekoliko najznačajnijih pristupa klasifikaciji ugrožavanja informacijskih sistema. Prikazom ovisnosti upotrijebljenih materijalnih nosilaca podataka i osjetljivosti na ugrožavanje želi se skrenuti pažnja na potrebu usklađivanja mjera zaštite, važnosti podatka, organizaciju informacijskog sistema i korištenje materijalnih nosilaca podataka.

Materijalni nosioci podataka; informacijski sistem; čuvanje; zaštita.

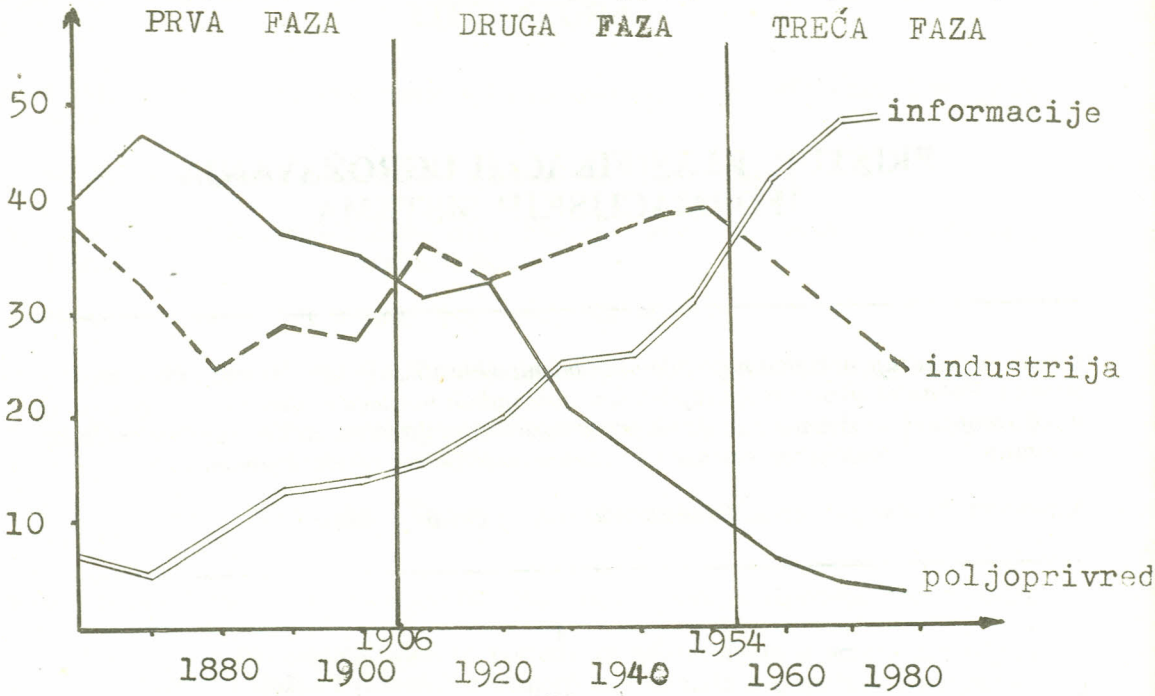
I

Nije potrebno posebno dokazivati da informacija postaje vrlo važan faktor u ljudskoj djelatnosti. Ona je podloga, prije svega, za poslovno odlučivanje i praćenje tehnološkog procesa a nezaobilazna je i kod samoupravljanja. "Međusobna uslovljenost i povezanost pojedinih dijelova međunarodne zajednice i rušenja tehničkih i drugih prepreka za širenje informacija među zemljama i kontinentima naše planete, pa i šire, uslovljavaju potrebu proučavanja širenja informacija i izgradnje sistema informisanja, ne izdvojeno u jednoj zemlji, već i međunarodnoj zajednici."(5) Razvoj naše zemlje dosegao je onu točku preko koje se lako neće moći preći ukoliko se ne poduzmu radikalne promjene u sferi prijenosa, obrade i korištenja informacija kao i u odnosu prema njima. Na primjeru danas informatički najrazvijenijih zemalja (a te su zemlje također u vrhu ljestvice ekonomski najrazvijenijih zemalja), uočljiva je preorijentacija iz industrijske i poljoprivredne proizvodnje u sferu proizvodnje i korištenja informacija i informatičke tehnologije. Ovu tvrdnju lijepo ilustrira Poratov dijagram kojim se pokazuje promjena u strukturi zaposlenih.(8)

Prema najnovijim podacima danas se 71,5% radnika bavi informatičkim poslovima, 25% radi u industriji, a samo 3,5% u poljoprivredi. (6)

Kod nas je prisutna sve veća brzina poslovnih promjena, a to uvjetuje i prati adekvatna informacijska podloga. Dinamiku promjena prati i tempo nastajanja informacija kojih je sve više, dinamičnije se smjenjuju pa se nameće potreba rješavanja probleme čuvanja i zaštite. "Društva i zajednice koji nisu mogli, ili nisu znali, osigurati pohranjivanje, razmjenu i korištenje svojeg intelektualnog vlasništva,

nisu mogli sačuvati ni svoj društveni status i kulturni identitet i nužno su propali i nestali."(9)Suvremena informatička tehnologija, tj. informacijski sistemi podržani



Slika 1.

kompjutorom, upotreba mikrofilma ili videodiska, olakšava rješavanje mnogih prije spomenutih zahtjeva. Uvjet za to je suvremeno koncipiran i tehnički dotjerano dizajniran informacijski sistem. Koncepcija takvog sistema u prvi plan stavlja procjenu značenja informacija i podataka koji se koriste u informacijskom sistemu, a time se određuju i kriteriji čuvanja i zaštite.

Informacije postoje da bi se koristile u komunikacijskom sistemu te predstavljaju njegovu osnovu i pretpostavku postojanja

u ostvarivanju komunikacijskih procesa. Komuniciranje nije jednosmjerni, a najčešće ni jednokratni proces. Da bi se omogućilo i osiguralo komuniciranje u prostoru i vremenu, potrebno je da informacije budu pohranjene i sačuvane za planirani vremenski period uz neprekidnu dostupnost njeznom sadržaju.

II

Pod pojmom čuvanja informacija podrazumijevaju se mjere i postupci kojima se osigurava ponovno pronalaženje informacija u zadanom vremenskom periodu. Zaštita informacija predstavlja niz mjera i postupaka kojima se informacije štite od

uništenja ili otuđenja u okviru procijenjenih oblika ugrožavanja. Primijenjeni oblici i metode ugrožavanja različito utječu na pojedine materijalne nosioce podataka. Zbog toga su postupci zaštite primjereni važnosti sadržaja i upotrijebljenom materijalnom nosiocu podataka, odnosno njegovoj otpornosti prema ugrožavanju.

Pristup klasifikaciji ugrožavanja informacijskog sadržaja je različit u zavisnosti o autorima koji izvode podjelu i namjenu klasifikacije. Neki autori, kao osnovu za klasifikaciju ugrožavanja sadržaja, uzimaju stupanj tajnosti informacija i s tim u vezi procjene prisutnog rizika.(1) U tom slučaju mjere zaštite poduzimaju se jedino ako je procijenjeni rizik velik, a moguće štete su veće od ulaganja u zaštitu informacijskog sadržaja. Procjena rizika je ipak podložna subjektivnom pristupu koji se u nekoj mjeri može svesti na prihvatljiv utjecaj, ali rizik se s vremenom mijenja u zavisnosti o sadržaju koji je prisutan u informacijskom sistemu.

Drugi u literaturi prisutan pristup klasifikaciji ugrožavanja informacijskog sistema je preko grešaka koje mogu biti hardverske, softverske, ljudske te prirodne nepogode.(4) Takav pristup nudi kao rješenje totalitarni sistem zaštite, kako bi se eliminirali svi oblici ugrožavanja. Cijena, danas nezanemariva komponenta u procjeni takve zaštite, vrlo je velika jer se pretpostavlja zaštita svakog informacijskog sistema bez obzira koji je značaj sadržaja i kakve bi štete prouzročio njegov gubitak.

Neki autori ugrožavanje informacijskog sistema svode na greške i propuste, zlonamjeran pristup i neovlašteno korištenje informacija te prirodne nepogode.(2) Bez detaljnijeg raščlanjivanja mogu se pretpostaviti utjecaji pojedinih izvora ugrožavanja na sadržaj i opremu, ali se teže može planirati zaštita. U tu svrhu potrebno je definirati načine kojima bi mogla biti ugrožena oprema, a posebno koji bi bili oblici i koje metode ugrožavanja sadržaja.

Postoji, u literaturi, pristup identifikaciji rizika preko opasnosti koje prethode nastanku štetnih događaja. Tako se dobiva detaljan prikaz oblika ugrožavanja informacijskog sadržaja, kao i prateće opreme, a taj zapostavlja izvore ugrožavanja u korist pragmatičnom pristupu u postavljanju mjera zaštite.(11)

Svođenje informacijskog sistema na njegove elemente hardware, software i kadrove, uz prikaz posljedica nastalih njegovim ugrožavanjem, ne ukazuje na oblike ugrožavanja, a ni na njihove izvore, pa zato otežava zaključivanje o mogućnostima uspješne zaštite.(8)

Kada se govori o ugrožavanju informacijskog sadržaja, treba razlikovati izvore ugrožavanja, oblike ugrožavanja te moguće metode ugrožavanja. Izvori ugrožavanja mogu biti navedeni kao: priroda kao izvor ugrožavanja, čovjek svjesnom i nesvjesnom svojom djelatnošću i tehničke greške nastale na opremi i objektima.

Priroda, kao izvor ugrožavanja, može ugroziti informacijski sadržaj djelovanjem elementarnih nepogoda. Tu treba spomenuti: poplave, potrese, požare velikih razmjera, elektromagnetska pražnjenja, klizanje zemljišta, odrone kamenja, zemlje ili snijega, djelovanje glodara, bakterija, gljivica itd. Mjere zaštite, koje se mogu poduzimati u ovom slučaju, spadaju u tehničke mjere zaštite i tako ih treba organizacijski tretirati.

Čovjek, nenamjernim djelovanjem, može biti jedan od aktera ugrožavanja informacijskog sistema. Tu su prisutni: neznanje, nepažnja, neodgovornost i nedisciplina. Ove atribucije odnose se na osoblje koje radi na održavnanju informacijskog sistema ili prateće tehničke opreme. Te mjere zaštite spadaju u kategoriju organizacijsko-edukativnih mjera. Treba ih definirati i od vremena do vremena kontrolirati.

Oblici ugrožavanja, koji stoje na raspolaganju kada svjesno djeluje u cilju ugrožavanja sadržaja, raznoliki su i ne mogu se svi nabrojiti. Tu se mogu naći: krađa važnih ili tajnih informacija, brisanje sadržaja, izmjena sadržaja, korištenje sadržaja u privatne svrhe, ratna djelovanja koja se manifestiraju kroz razaranja, požar, poplave, radijacija ili otuđenje opreme i sadržaja, elektromagnetsko zračenje velikog intenziteta, povišena temperatura-požar, čestice prašine, štetni plinovi, nepoštivanje propisanih procedura u tehnologiji rada i sl. Mjere, kojima se mogu spriječiti ovakvi oblici ugrožavanja, jesu organizacijsko-softverske prirode.

Tehničke greške kao izvore ugrožavanja mogu ilustrirati ovim pojavnim oblicima: rušenje zgrada zbog grešaka u statičkim proračunima; hardverske greške koje nastaju u radu opreme, greške u jedinicama eksternih memorija, u komunikacijskim linijama; softverske greške, krivo izrađeni programi, problemi u toku testiranja i implementacije novih programa, greške u kreiranju datoteka, greške u sistemskom programu, nedostatak zaštitnih rješenja, kvar u sistemu dojave požara, gubitak napona i mogućnosti paralelnog napajanja ili njegove neispravnosti isl.

Objekti ugrožavanja u informacijskom sistemu mogu biti tehnička sredstva podrške sistema ili same informacije. Ako se radi o oblicima ugrožavanja informacija sa zaštitinog aspekta, tada se oni mogu podijeliti na oblike ugrožavanja sadržaja i ugrožavanje materijalnih nosilaca podataka.

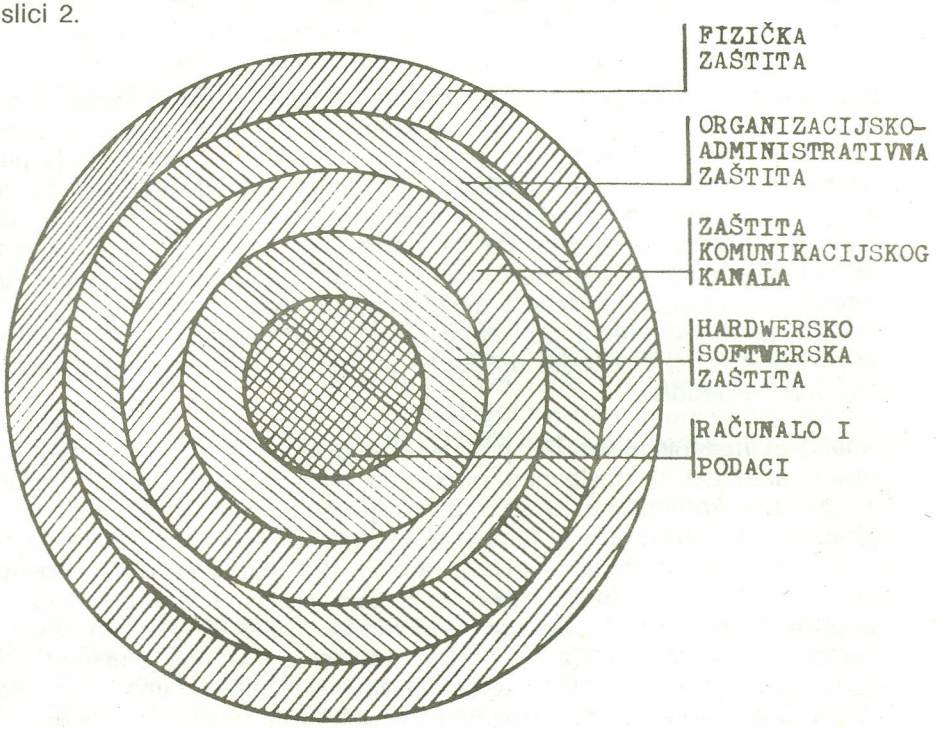
Učestalost pojedinih oblika ugrožavanja već se duže vremena prati kako bi se stvorili korisni zaključci za izradu optimalnih načina zaštite. Britanski izvori pokazuju slijedeću distribuciju oblika ugrožavanja: (6)

- krađa opreme	25%
- požari i bombe	20%
- sabotaža	20%
- krađa informacija	13%
- otvoreno oštećenje	10%
- prodiranje u sistem	10%
- logičke "bombe"	2%.

Iz ovakvog pregleda može se zaključiti kakva je učestalost pojedinih oblika ugrožavanja, te se potrebnom obliku zaštite može pridati veći stupanj prioriteta . Štete, nastale zbog kompjuterskog kriminala, nisu male, te se raspolaže podatkom da je osamdesetih godima u Engleskoj šteta od kompjuterskog kriminala bila 500 milijuna funti, a da je to samo 15% stvarnih šteta.

U ovom radu ne mogu se tretirati sve moguće mjere zaštite jer to mu nije ni cilj, niti mu to opseg omogućava. U tekstu su naznačene samo neke mjere zaštite uz

pojedine oblike ugrožavanja. Ilustrativnije se to može grafički prikazati kao što je to učinjeno na slici 2.



Slika 2.

Za potrebe prakse, da bi se odredili odgovarajući oblici zaštite, potrebno je izračunati tehničku sigurnost informacijskog sistema. Nažalost, sigurnost u koju se uključuje i ljudski faktor vrlo je teško odrediti, zbog čega ne postoje ni pouzdani obrasci. Tehnička se sigurnost izračunava umnoškom pouzdanosti (pi) koju posjeduju pojedini elemenati, a čine niz u međusobnoj zavisnosti. Matematički se tehnička sigurnost izražava slijedećim obracem:

Da bi se postigla veća pouzdanost funkcije sistema, rizični elementi sistema

$$P = \prod_{i-1}^{n} (p_i)$$

postavljaju se u višestruko paralelnom spoju, ako je to moguće, te se u tom slučaju pouzdanost (pi) elementa izračunava:

$$p_i = 1 - q_i, i = 1,2,...,n,$$

gdje je $p+q=1$, tj. zbroj pouzdanosti i nepouzdanosti elemenata sistema jednak jedinici, dok je n broj elemenata o paralelnom spoju.

III

Obrađuje li se pitanje čuvanja i zaštite podataka i informacija u suvremenom informacijskom sistemu, tada se najćešće misli na informacijski sistem podržavan računalom. Takav je pristup prisutan i u ovom radu, ali potrebno je nešto reći i o čuvanju i zaštiti podataka u sistemu transefra i obrade informacija bez podrške računala. Jasno je da se tada misli na informacijski sistem u kojem je papir osnovni materijalni nosilac podataka, pa se pažnja kod kreiranja mjera čuvanja i zaštite usmjerava na njegove karakteristike i prateća organizacijska rješenja. Pažljiv odabir materijalnog nosioca podataka može olakšati probleme zaštite sadržaja jer im je različita otpornost prema pojedinim oblicima ugrožavanja. Kao najčešće korišteni materijalni nosioci podataka danas se susreće papir, elektromagnetska memorija, mikrofilm i videodisk.

Papir, kao materijalni nosilac podataka, pojavljuje se kao dokument ili uobičajeni nosilac sadržaja u poslovnim odnosima, kao bušena kartica, bušena traka ili listing-izlaz iz kompjutora. Zbog lake zapaljivosti poželjno je čuvati papirnate nosioce podataka u prostoru gdje je temperatura 20-25 C. Kod temperature od 140 C dolazi do djelomičnog uništenja sadržaja, a kod 170 stupnjeva do njegovog potpunog gubitka. Poželjna vlažnost zraka je 20-65% relativne vlažnosti kao optimum za dugotrajno čuvanje. U slučaju izloženosti papira direktnom djelovanju vode informacijski sadržaj, koji je bio zapisan na papiru, potpuno je uništen. Dim i prašina ne utječu na papir u smislu uništenja zapisa ili bitnog smanjenja vijeka trajanja medija. Osjetljivost papira na mehanička oštećenja relativno je velika.

Elektromagnetske memorije, koje se koriste kao eksterne memorije, jesu: magnetska traka, kartica i magnetski disk. Zajedničko im je obilježje što su od poliesterske ili metalne podloge presvučene s feromagnetskim materijalom koji služi za upisivanje podataka. Osjetljivost na temperaturu je izražena djelomičnim gubitkom zapisa kod izloženosti medija temperaturi od 65 C. Potpuni gubitak zapisa nastaje već kod 100 C. Kod trake poželjna relativna vlažnost zraka iznosi 20-60%, a kod diska 5-95% relativne vlažnosti. Direktno djelovanje vode uništava medij i zapis, s tim da je čitljivost trake moguća još nekoliko dana nakon sušenja s velikom mogućnošću grešaka u čitanju zapisa. Dim i prašina ne štete mediju, ali njihove naslage mogu oštetiti glave čitača prilikom čitanja zapisa. Magnetske memorije osjetljive su na elektromagnetska zračenja bilo kakvog porijekla. Iste efekte, gubitka sadržaja, izaziva i radijacija. Osjetljivost na mehanička oštećenja je prisutna, iako nije posebno izražena, osim ako ne dođe do skidanja ili oštećenja feromagnetskog sloja.

Mikrofilm se, kao materijalni nosilac podataka, pojavljuje u tri različite forme: srebro-halogeni sloj na poliesterskoj podlozi, diazo i vezikular. Osjetljivost mikrofilma na temperaturu je vrlo velika tako da je kod srebro-halogenog optimalna temperatura pohrane 20-25 C, a kod diazo ili vezikulara maximalno 21 C. U zavisnosti kakva je podloga mikrofilma opasnost od gorenja je različita. Temperatura oko 90 C u pravilu uništava snimljeni sadržaj na mikrofilmu. Za razliku od osjetljivosti na temperaturu, otpornost mikrofilma na vlagu je velika. Voda može utjecati na srebro-halogeni sloj pa dolazi do oštećenja snimke ali zato ne utječe na diazo ili vezikular mikrofilm koji

se može nakon sušenja normalno koristiti. Dim i prašina ne utječu na mikrofilm. Prisutna je stanovita osjetljivost želatine srebro-halogenog filma na plinove u dimu koji bi mu mogli smanjiti vijek trajanja. Mikrofilm, kao medij, osjetljiv je na mehanička oštećenja, posebno ogrebotine, jer se zbog velike gustoće zapisa gubi mnogo sadržaja.

Videodisk je tek u fazi uvođenja i koristi se kao medij čuvanja i pohrane informacija. Pored svih prednosti koje nudi nije našao širu primjenu zbog tehničkih nesavršenosti. Osim što je on nereverzibilna memorija, nastoji se svesti vjerojatnost greške ili gubitka dijela sadržaja na red veličine 10 na - 10, prije nego se uvede u uredsko poslovanje ili kao eksterna memorija u informacijskom sistemu podržanom računalom. Postojanost i čitljivost zapisa na videodisku zavisi o vrsti odabranog diska i iznosi u prosjeku oko 10 godina. Zbog velike gustoće zapisa značajan problem predstavlja čuvanje medija od prašine, jer zrnce prašine pokriva veliko područje zapisa i čini ga nečitljivim. Utjecaj vlage ne odražava se na kvalitetu zapisa ili mogućnost čitanja, ali voda unosi nečistoću i onemogućava čitanje. Osjetljivost ovog medija na povišenu temperaturu je izražena.(1)

IV

Mjere zaštite i čuvanja informacija i podataka mogu biti raznovrsne. Odluka o njihovom odabiru prije svega ovisi o procjeni važnosti sadržaja i njegove praktične iskoristivosti, ali i o subjektivnom odnosu projektanta informacijskog sistema prema tom segmentu projektiranja. Društvena potreba za egzaktnom podlogom u donošenju odluka u svim sferama društvene djelatnosti i svim nivoima odlučivanja može mnogo doprinijeti bržoj promjeni shvaćanja važnosti informacija i potrebi njihovog čuvanja i zaštite.

U našim uvjetima, uvjetima materijalne oskudice, privredne nepropulzivnosti i posljedica na društvene odnose trebalo bi što prije staviti relevantnu, točnu i ažurnu informaciju u prvi plan samoupravnog, poslovnog i političkog odlučivanja. Takav zahtjev može ispuniti suvremena informatička oprema. Prelazom na automatsku obradu podataka i informacija ne mogu se zapostaviti i zanemariti prije korištena rješenja i metode rada. Trebat će stvoriti "most", prije svega u sferi čuvanja i zaštite podataka, s prije važećom organizacijom informacijskih sistema i upotrebljavanim materijalnim nosiocima podataka. Nova rješenja trebaju respektirati prije korištene metode rada, materijalne nosioce podataka i informacija i omogućiti korištenje informacijske osnove s pronalaženjem podataka na materijalnim nosiocima potuno različitih karakteristika i načina pristupa do informacije.

Kod projektiranja informacijskih sistema u segmentu čuvanja i zaštite treba utvrditi mjere koje će se s tim ciljem poduzimati. Uprkos tome, što je potrebno osigurati dostupnost informacija i podataka, mjere čuvanja i njihove zaštite usmjerene su na zaštitu materijalnih nosilaca podataka. Sadržaj informacija utjeće samo na odluku o potrebi čuvanja ili zaštićivanja sadržaja.Izvori ugrožavanja informacijskog sadržaja orijentirani su prema ugrožavanju informacija, a oblici i metode ugrožavanja, preko kojih se može postići željeni cilj, orijentirani su na materijalne nosioce podataka.

Zaštitom materijalnih nosilaca podataka zapravo štitimo informacijske sadržaje koji se na njima nalaze.

LITERATURA

1. BASIĆ D., Kako zaštititi kompjuter, Basić, Zemun, 1988.
2. CAREVIĆ M., Osnove elektroničke obrade podataka i njena primjena u izgradnji informacijskog sistema, organa unutrašnjih poslova, Republički sekretarijat za unutrašnje poslove, Zagreb, 1986.
3. GRUPA AUTORA, Kriza, blokade i perspektive, Globus, Zagreb, 1986.
4. MUFTIĆ S., Sigurnost kompjutorskih sistema, Zavod za ekonomsko planiranje Sarajevo, Sarajevo, 1979.
5. OREČ M., Osnovi sistema informisanja, Privredni pregled Beograd i Oslobođenje Sarajevo, Sarajevo, 1977.
6. PETROVIĆ S., ĆIRIĆ V., Zaštita podataka u automatizovanim informacionim sistemima, Naučna knjiga, Beograd, 1986.
7. PLEVNIK D., Informacija je komunikacija, Radna zajednica Centra društvenih djelatnosti SSOH, Zagreb, 1986.
8. SRIĆA V., Budućnost pripada informatici, Radna zajednica Centra društvenih djelatnostu SSOH, Zagreb, 1984.
9. TUĐMAN M., Teorija informacijske znanosti, Informator, Zagreb, 1986.
10. TURK I., DEŽELJIN J., Organizacija informacijskog sistema, Informator, Zagreb, 1977.
11. TURK I., DEŽELJIN J., Tehnike osiguranja računskog centra i zaštite podataka - podsjetnik, Intertrade, Radovljica, 1984.
12. TURK I. DEŽELJIN J., Problematika zaštite u informatičkoj djelatnosti Savjetovanje u Medulinu 2-5. III 1987., Andragoški centar, Zagreb, 1987.

Primljeno: 1989-09-16

Hutinski Ž. Die Klassifikation der Gefaehrdung der Informationssysteme

Zusammenfassung

In der vorliegenden Arbeit beschreibt man die wichtigsten Betrachtungsweisen der Klassifikation der Gefaehrdung der Informationssysteme. Die Auswahl der materiellen Datentraeger muss bei der Projektierung der Informationssysteme ausser der informations-kommunikativen Rechtfertigung die Bedingung der Aufbewahrung und des Schutzes rechtfertigen.

(Prijevod: Vesna Šimunić)