Revija za kriminalistiko in kriminologijo | Ljubljana 33 | 1982 | 2

UDK 343.3/.7:681.3

Pojavne oblike zlorabe računalnika

Bogo Brvar*

I. UVOD

1. Računalništvo, informatika, informacijski sistem

Človeško znanje je v eksploziji. Prvič se je glede na vse predhodno znanje in vsa znanstvena odkritja podvojilo v tem stoletju, med leti 1900 in 1950. Že v naslednjih letih, do leta 1960, pa je prišlo do ponovne podvojitve. Po raziskavah univerze v Stanfordu v ZDA bo prihajalo do podvajanja znanja v vse krajših razdobjih, od 6 do 8 let.[1] Zelo hitro se je razvila znanstvena disciplina **informatika,** ki je prav tako hitro napredovala v znanstveno vedo, vsaj takšen status ji daje večji del znanstvenih delavcev, ki proučuje področja njenega raziskovanja. Vsekakor pa informatika ni samo znanstvena veda, ampak je to predvsem veda dejanskosti, uporabna veda.

Pojem informatika je nastal z združitvijo besed informacija in avtomatika na francoskem govornem področju (INFORmation + autoMATIQUE).[2] Zanjo obstaja več definicij. Najkrajša jo definira kot vedo o informacijah, njihovem oblikovanju, prenosu, zapisu, obdelavi in uporabljanju,[3] širša definicija pa pravi, da je **informatika veda, ki združuje vsa področja, ki se nanašajo na načrtovanje, gradnjo, uporabo in vzdrževanje sistemov za obravnavanje informacij, vključujoč aparaturno in programsko računalniško opremo, organizacijske in človeške vidike ter njen celovit vpliv na proizvodno, poslovno, upravno-administrativno, družbeno in politično območje.**[4] Delimo jo v tehniko informatike in uporabno informatiko. **Tehnika informatike** obsega računalniške vede, ki jih kratko imenujemo **računalništvo, uporabna informatika,** ki jo kratko imenujemo **informatika,** pa obsega proizvodno, poslovno-administrativno, družbeno, biomedicinsko in tehnično informatiko.[5]

Razvoj računalništva je, gledano z očmi povprečnega človeka, skoraj neverjeten. Izdelovalci računalniške opreme napovedujejo novo generacijo računalnikov, ki naj bi še bili grajeni na osnovi »klasične« tehnologije, ni pa daleč čas, ko bo sedanja ultraminiaturna vezja zamenjala nova tehnologija, pomnilniki z magnetnimi mehurčki in elektronskim žarkom. Število enot podatkov, ki jih sprejmejo centralni pomnilniki novih računalnikov, že presegajo število enot, ki so jih sprejeli direktni eksterni spomini računalnikov, izdelani pred nekaj leti. Računalnik in vse, kar je povezano z njim, ima ogromen vpliv na razvoj človeštva. In s časom bo ta vpliv še naraščal po eksponentni funkciji. Je pa pozitiven in negativen. Na eni strani je njegova uporaba ogromno pripomogla k širjenju znanja, saj je z njim mogoče v nekaj sekundah ali celo delih sekunde opraviti nekaj deset milijonov matematičnih in primerjalnih operacij in simulirati postopke, ki se v naravi odvijajo nekaj mesecev ali nekaj let. Na drugi strani pa prihaja do lastništva ogromnega števila podatkov s katerimi si industrijsko razviti svet ustvarja ekstraprofite, ko te podatke v obliki tehnološkega postopka prodaja manj razvitemu in nerazvitemu svetu oziroma izkorišča njegovo delovno silo in naravna bogastva. Boj revnega juga z bogatim severom je v veliki meri boj za pravičnejšo porazdelitev informacij v najširšem smislu besede.

Hiter razvoj tehnike informatike, ki je prispeval k hitremu razvoju uporabne informatike, je zahteval sistemski pristop k obravnavanju vseh vprašanj v zvezi z obdelavo in prenosom podatkov. Tak pristop pa je pripeljal do razvoja **informacijskih sistemov,** sistemov, ki v organizaciji, ustanovi, pokrajini ali državi opravljajo **vse naloge v zvezi z zapisovanjem, shranjevanjem, obdelavo, iskanjem, izkazovanjem in prenosom podatkov.**[6] Sestavljajo ga ljudje-subjekti, ki sistem gradijo in ga uporabljajo, **tehnična sredstva** (celotna računalniška oprema in komunikacijska sredstva), ki so materialna osnova sistema, in **organizacijski postopki, metode in načini** usklajevanja in povezovanja vseh elementov v funkcionalno celoto, vključno s programsko opremo (nematerialna osnova sistema).[7] Glede na smer kroženja podatkov v sistemu, glede na dolžnosti in pravice subjektov sistema in glede na razporeditev tehničnih sredstev delimo informacijski sistem v štiri dele — štiri skupine aktivnosti: vhod (input), izhod (output), obdelavo (processing) in povratno vezo (feedback). V manjših, zaprtih informacijskih sistemih so ti deli bolj strogo ločeni med seboj kot v večjih, odprtih, dinamičnih sistemih, v katerih sta vhod in izhod glede na subjekte, tehnična sredstva in lokacijo pogosto skoraj identična.

* Prof. matematike in fizike, Višja šola za notranje zadeve.

[1] Srića, s. 2.
[2] Ferišak in drugi, s. 6.
[3] Prav tam.
[4] Virant, s. 5.
[5] Prav tam.
[6] Prav tam.
[7] Ferišak in drugi, s. 51.

Vhod je tisti del sistema, ki opravlja nalogo zbiranja, evidentiranja in vnosa podatkov v računalniško bazo podatkov.[8] Pri teh opravilih se lahko uporabljajo daljinske računalniške enote — terminali, ki omogočajo direkten vnos podatkov v računalnik iz poljubne lokacije, ali pa se celoten postopek odvija še klasično, preko vhodnih formularjev.[9] Vhod je lahko porazdeljen in se odvija na več mestih delovnega območja nosilca informacijskega sistema, lahko pa je centraliziran in poteka na eni ali dveh lokacijah (manjši zaprti informacijski sistemi nekaterih organizacij združenega dela).

Uspešno opravljanje del pri vhodu ne zahteva posebnega znanja iz računalništva, delavec mora poznati le tisti del uporabne informatike, ki obsega že zgoraj omenjene postopke: zbiranje, evidentiranje in vnos podatkov v računalniško bazo podatkov.

Obdelava obsega hranjenje informacij in podatkov na magnetnih medijih in računalniško obdelavo na zahtevo upravičenega uporabnika, skupaj s pripravo in oblikovanjem izhodnih informacij. Včasih so lahko aktivirali obdelavo in vplivali na njen potek samo delavci, ki so bili v neposredni bližini računalnika — v računskem centru. Sodobne interaktivne metode pa so to centralizacijo povsem decentralizirale, saj je teoretično in praktično možno iz kateregakoli terminala, ki je povezan z računalnikom, aktivirati obdelavo.

Od nalog, ki jih opravlja delavec v obdelavi, je odvisna stopnja potrebnega znanja iz računalništva in informatike.

Izhod je tisti del sistema, po katerem se navadno meri kakovost informacijskega sistema. Ostre meje med obdelavo in izhodom ni, to še posebej velja za sisteme, ki imajo porazdeljen direktni izhod. Zajema prenos informacij iz računalnika in njihovo uporabo v najširšem smislu besede. V njem sodelujejo subjekti informacijskega sistema, pa tudi subjekti okolice.

Stopnja strokovnega znanja uporabnika izhodnih informacij je odvisna od njegovih zadolžitev. Tisti, ki jih neposredno uporabljajo, prvi prejemniki, morajo imeti predvsem dovolj znanja iz uporabne informatike, s področja, na katerem delajo.

Povratne veze zagotavljajo stalno vrednotenje informacijskega sistema. To so podatki o kakovosti, uporabnosti izhodnih informacij in sploh o delovanju sistema. Na podlagi kritike izhodnih informacij se lahko menja njihov obseg in oblika, pa tudi vhod, obdelava in vsebina baze podatkov. Povratne veze pomenijo interakcijo med vhodom in izhodom in na ta način povezujejo vhod, izhod in obdelavo v sklenjen sistem.

Povratne informacije so izražene eksplicitno ali pa jih dobimo z razčlembo učinkovitosti informacijskega sistema oziroma njegovega podsistema.

Informacijski sistemi uporabljajo **digitalne računalnike,** ki operirajo izključno s števili.[10] V industriji, prometu, raziskavi materiala, energetiki in podobnih panogah pa se uporabljajo **analogni računalniki,** ki števila pretvarjajo v fizikalne količine (vodenje avtomatiziranih delovnih postopkov, upravljanje sistema semaforjev itd.).

2. Definiranje kriminalitete v zvezi z računalniki

V sodobnem svetu kriminaliteta dokaj hitro menja svojo obliko. Nekatere vrste kaznivih dejanj izginjajo, nastajajo nove, drugačne so oblike in tehnika izvedbe, menjajo se motivi. Tudi v kriminaliteti se uporabljajo dosežki znanosti in tehnike. Tako v njej vedno bolj pogosto srečamo uporabo tehnike informatike, pa tudi znanja iz uporabne informatike. V svetu govorijo o računalniškem kriminalu. Gre za **kriminaliteto v zvezi z računalniki.** Pojem računalniška kriminaliteta je sporen, ne glede na to, da na zahodu že več kot 20 let govorijo o computer crime.

Če bi namreč osvojili pojem računalniška kriminaliteta, bi v kriminologiji klasificirali kriminaliteto po uporabljenem sredstvu pri izvrševanju kaznivih dejanj, kar pa do sedaj ni bila praksa (sicer ne gre samo za kazniva dejanja z uporabo računalnika, so pa najbolj pogosta). Res je, da je kriminološka tipologija v primerjavi z legalno dinamična in se prilagaja novim pojavnim oblikam kriminalitete, vendar pa bi s tipologijo kriminalitete po uporabljenih sred-

[8] Pod računalniško bazo podatkov razumemo sistem vseh memoriranih podatkov, s katerimi upravlja informacijski sistem.

[9] Večji del informacijskih sistemov uporablja tako direktni vnos podatkov v računalnik (on-line oblika povezave), kot tudi še izpolnjevanje vhodnih formularjev in nato prenos teh do računalnika, kjer se podatki šele vnesejo vanj (off-line oblika povezave).

[10] Digitalni računalniki razpoznavajo samo dve stanji: DA in NE, ki ju reprezentirajo z 0 in 1. Vsi podatki in ukazi so v računalniku predstavljeni s tema dvema številoma — z binarnim številčnim sistemom.

stvih naredili preveliko zmedo, ker bi lahko naenkrat govorili o brezštevilnih kriminalitetah. Po drugi strani tudi računalnik sam kot tak še ni storil kaznivega dejanja in ga nikoli ne bo. Kako bogata je po obsegu in raznolikosti kriminaliteta, pri kateri je tako ali drugače uporabljen avto, brez upoštevanja kaznivih dejanj v prometu, pa ne govorimo o avtomobilski kriminaliteti.[11] Računalnika kot enega največjih tehnoloških dosežkov človeka ne primerjamo z avtomobilom, vsaj danes ne, ko je avto nekaj vsakdanjega; vendar pa je tudi računalnik **samo orodje v človekovih rokah.** Zato je verjetno najbolj pravilno, da govorimo o **kriminaliteti v zvezi z računalniki**[12] ali morda o **kriminaliteti z računalniki.**

Definicij zanjo je več. V literaturi beremo, da je to:

— uporaba računalnika pri izvedbi goljufije, utaje in zlorabe, katere namen je pridobiti lastnino, denar ali uslugo, ter pri politični in poslovni manipulaciji; vključuje tudi dejanja, naperjena proti računalniku samem;[13]

— kriminaliteta, sestavljena iz kaznivih dejanj, v katerih se računalnik pojavlja **kot orodje ali kot cilj** (tarča);[14]

— izvajanje prepovedanega dogajanja v računalniku;[15]

— oblika kriminalitete belega ovratnika, ki se dogaja s pomočjo računalniških sistemov;[16]

— uporaba računalnika pri izvrševanju kaznivih dejanj.[17]

Izmed teh definij se najbolj približa bistvu tista, ki govori o računalniku kot orodju in cilju kaznivega dejanja, vendar pa jo je treba dopolniti. Sem ne moremo šteti kaznivega dejanja, ki ga stori jezna ali alkoholizirana oseba, ko vrže steklenico v računalnik in ga s tem poškoduje, ni pa imela v svoji zavesti najmanjšega namena poškodovati prav računalnik (v trenutku »jeze« je bil pač najbližji objekt). Enako velja za tatvino računalnika, ko storilcu ni treba storiti nič več, kot če bi ukradel televizor (storilec, ki vlomi v prostor z računalnikom in odnese vse, kar se da, mogoče sploh ne ve, da je vlomil v računalniški center).

Vsekakor mora definicija za kriminaliteto v zvezi z računalnikom vsebovati sestavino — **pogoj, ki mora biti izpolnjen, da kaznivo dejanje v zvezi z računalnikom** (uničenje, poškodovanje, tatvina) ne štejemo med običajno kriminaliteto. **Storilec mora imeti namen in vzrok za poškodovanje oziroma tatvino računalnika ali kakšnega njegovega dela, in ta vzrok mora imeti svoj izvor v kaki računalnikovi lastnosti. Če pa storilec to lastnost pozna, mora imeti določeno znanje iz računalništva, računalniške tehnologije ali uporabe računalnika.**[18] Tako lahko definiramo kriminaliteto v zvezi z računalniki **kot kaznivа dejanja, v katerih se pojavlja računalnik kot sredstvo (orodje), predmet ali objekt napada, za izvršitev ali poskus izvršitve kaznivega dejanja pa je potrebno določeno znanje iz računalništva (tehnika informatike) ali informatike (uporabna informatika).**

Dvomov ni. Tudi oseba, ki ničesar ni vedela o računalništvu ali informatiki, je pa slišala, da so v računalniku hranjeni določeni podatki o njej, to pa njej ni po volji in ob priložnosti poškoduje računalnik, v tem trenutku ima določeno znanje o računalniku in sicer to, da so v njegovem spominu hranjeni podatki. Vzrok poškodovanja je v zvezi z lastnostjo računalnika.

Glede na to, da mora biti izpolnjen osnovni pogoj — določeno znanje iz tehnike informatike in uporabne informatike, morda lahko kriminaliteto v zvezi z računalniki imenujemo **kriminaliteto v informatiki.** Dejansko je to bolj točen pojem, saj pogosto ne gre za znanje iz računalniških ved, računalniške tehnologije, ampak za znanje iz uporabne informatike. Verjetno se bo ta pojem v prihodnosti pokazal kot pravilen.

Najbolj razširjena in kriminološko najbolj zanimiva so dejanja, v katerih se računalnik uporabi kot sredstvo. To vrsto kriminalitete v zvezi z računalniki imenujemo **zlorabo računalnikov.** Kazniva dejanja, pri katerih se računalnik pojavlja **kot predmet,** so redka. Literatura ne navaja posameznih primerov.[19] Tretja vrsta pa so

[11] Verjetno se je kdaj pisalo ali govorilo tudi o avtomobilski kriminaliteti, toda pojem se ni uveljavil.

[12] Tudi zahodni avtorji v zadnjem času pišejo predvsem o computer-related crime (kriminaliteta v zvezi z računalniki) in ne o computer crime.

[13] Bequai, Computer crime, s. 4.

[14] Prav tam.

[15] Computer crime, Criminal Justice Resource Manual, s. 4.

[16] Prav tam, s. 5.

[17] Prav tam.

[18] Osnovni pogoj.

[19] Znana so kazniva dejanja (predvsem v ZDA), ko storilci vlamljajo v računalniške centre in odnesejo ali bolje odpeljejo računalnik in njegove enote, vendar gre predvsem za oblike klasičnih velikih tatvin, pri katerih ni izpolnjen osnovni pogoj. Drugo pa je seveda vprašanje, kaj se z računalnikom dogaja kasneje.

kazniva dejanja, pri katerih imajo storilci namen uničiti ali poškodovati računalnik in njegove enote, vključno s komunikacijskimi potmi — **objekt napada.** Ločiti moramo poškodovanje ali uničenje računalnika z namenom izbrisati — uničiti podatke, ki so v njegovem spominu, ali vsaj začasno onemogočiti dostop do njih in poškodovanje ali uničenje računalnika samega kot takega (sabotaža, vandalizem).

Kriminaliteto v zvezi z računalniki delimo torej po vlogi, ki jo ima računalnik v kaznivem dejanju.

II. POJAVNE OBLIKE

Vse do sedaj znane pojavne oblike zlorabe računalnikov lahko razvrstimo v tri večje skupine:

— zlorabo podatkov in informacij (v nadaljevanju: podatkov),

— zlorabo programske opreme in postopkov ter

— neupravičeno uporabo računalniške in programske opreme.

Ko govorimo o posameznih oblikah zlorabe računalnika, imamo v mislih digitalne računalnike, vsaj dosedanja praksa je takšna, čeprav zlorabe analognih računalnikov niso nemogoče. Nasprotno, posledice takih zlorab bi bile lahko zelo hude. Vzemimo zelo enostaven primer: avtomatizirano proizvodnjo določene vrste avtomobilskih delov. Kako tragične bi lahko bile posledice, če bi v računalniku spremenili navodila (programe), tako da bi vsakemu desetemu kosu spremenil strukturo prvin in s tem bistveno zmanjšal njegovo odpornost. Za sedaj tovrstnih kaznivih dejanj ne poznamo (ali pa jih ne znamo odkrivati), vsekakor pa po kriminološki klasifikaciji spadajo med zlorabo računalnikov.

Dejanja zlorabe računalnikov lahko nastajajo v kateremkoli delu informacijskega sistema, v katerikoli aktivnosti s tem, da ločimo **posredno** in **neposredno zlorabo računalnika.** O posredni zlorabi govorimo takrat, ko gre za dejanje glede aktivnosti vhoda, izhoda in povratne veze. Storilec pri tem lahko posega tudi v podatkovno bazo, vendar ne pozna njenega ustroja in pravil za njeno spreminjanje. Podatek namerno spremeni, ker ve, da računalnik ni tako programiran, da bi preveril pravilnost podatka, oziroma tega sploh ni mogoče preveriti. Pri posredni zlorabi ne gre nikoli za spreminjanje programov. Neposredna zloraba pa zajema kazniva dejanja v sami računalniški obdelavi.[20] Gre za neposreden poseg v podatkovno (manipulacija že memoriranega podatka) in programsko bazo. Tako pri neposredni kot pri posredni zlorabi pa mora biti izpolnjen osnovni pogoj.[21]

1. Zloraba podatkov

Kazniva dejanja zlorabe podatkov so v primerjavi z ostalima skupinama zlorab računalnika najštevilnejša, pa tudi najbolj raznolika. **Skupna značilnost vseh teh dejanj je takšno ali drugačno »ogrožanje podatkov«.** Zahodni avtorji to imenujejo »data crime«[22] — kriminal s podatki.

Med dejanja zlorabe podatkov štejemo:

— manipulacije s podatki (spreminjanje, brisanje, dodajanje napačnih — neupravičenih podatkov) in

— neupravičen dostop do podatkov (računalniško vohunstvo).

a) Manipulacije s podatki

Pri manipulacijah s podatki gre za vse oblike spreminjanja, brisanja in dodajanja napačnih oziroma neupravičenih[23] podatkov na vhodu — pred ali med vnosom v računalniški spomin, med obdelavo ali na izhodu, če je izpolnjen osnovni pogoj. Načini storitve so različni. Nasploh je za celotno **zlorabo računalnikov značilen zelo raznovrsten modus operandi.**[24] Odvisen je od stopnje razvitosti informacijskega sistema (čimbolj izpopolnjen je informacijski sistem, tako v organizacijskem, kadrovskem in tehničnem smislu, tem bolj zapleten in dovršen modus operandi lahko pričakujemo), od varovanja — zaščite informacijskega sistema ter od znanja storilca oziroma storilcev, če gre za organizirane oblike sodelovanja več oseb.

Najbolj enostavna oblika manipulacije s podatki je **namerno spreminjanje vsebin vhodnih formularjev** (med vpisovanjem podatkov v formularje, nadzorom vpisanih podatkov, šifriranjem) in spreminjanje podatkov med vnosom v računalnik (storilec **pravilno prečita ali sliši**

[20] V ožjem smislu: prepovedano poseganje v obdelavo, ki se trenutno odvija v računalniku — med izvajanjem programa.

[21] Glej opombo 18.

[22] Bequai. Organized Crime in the Computer Arena, s. 24.

[23] Podatek sam kot tak je lahko pravilen, ni pa upravičena njegova zabeležba na formularju ali v računalnikovem spominu.

[24] Zima, s. 1.

pravilen podatek, toda na luknjano kartico, magnetni trak, magnetni disk vnese popačen podatek[25]).

Če gre za manipulacijo s podatki, ki so že na magnetnih nosilcih, dostop do njih je torej možen izključno preko računalnika, govorimo o **manipulaciji memoriranih podatkov.** Do te lahko pride med dejansko obdelavo teh podatkov na računalniku (legalna obdelava) ali z nasilnim posegom (nelegalna obdelava) z namenom spreminjanja, brisanja ali dodajanja. Zadnji način storitve šteje med najbolj dovršene oblike zlorabe podatkov, ki pa se med seboj razlikujejo še **po zahtevnosti izvedbe. O lažji obliki govorimo ko gre za uporabo obstoječih vhodno-izhodnih enot** računalnika, bodisi da gre za poseg preko naprav, ki so v neposredni bližini memoriranih podatkov[26] (zelo omejen krog možnih storilcev), bodisi da gre za poseg preko daljinskih naprav — preko terminalov. Pri tem je pomembno še to, da storilec aktivira del programske opreme, ki omogoča uporabljanje in spreminjanje računalniške evidence. V te programe pa ne posega — jih ne spreminja, ampak jih samo uporabi.[27]

Osnovno (temeljno) dejanje je neupravičeno spreminjanje določenega stanja v računalniški evidenci, toda to dejanje navadno spremljajo še neupravičen dostop v računalniško evidenco (zloraba pooblastil), zloraba gesla-šifre, ki omogoča dostop, in morda celo kaznivo dejanje, s katerim je storilec prišel do gesla. Možne storilce je treba iskati med osebami, ki imajo možnost uporabljati računalniške vhodno-izhodne enote in posegati v računalniške evidence. Ne gre pa izključiti tudi drugih uporabnikov oškodovanega informacijskega sistema in celo zunanjih oseb. Teoretično in pogosto tudi praktično je možno poseči vsaj v eno računalniško evidenco iz vsake vhodno-izhodne naprave računalnika, ki je z njim povezana.

Bolj zahteven način storitve srečamo pri dejanjih, pri katerih gre za neupravičeno spremembo stanja v računalniški evidenci preko obstoječih vhodno-izhodnih enot računalnika, z **neupravičeno uporabo programske opreme,** ki jo je storilec **modificiral,** priredil za izvedbo svojega dejanja. Gre torej za prepovedano dejanje **manipulacije s programi in podatki.** Takšno dejanje uvrščamo med zlorabe podatkov, ker je manipulacija s programi pripravljalno dejanje za storitev glavnega kaznivega dejanja — spremembe stanja v računalniški evidenci.

Možna pa je še oblika kaznivega dejanja, pri katerem storilec preko obstoječega terminala z neupravičeno prirejenim programom prestreže sporočilo, informacijo, ki potuje na poti računalnik—terminal, in to informacijo spremeni, uniči ali ji doda drugo, lažno informacijo, ki bistveno spremeni vsebino prvotne informacije. Krog možnih storilcev je zelo ozek, saj mora storilec poleg uporabne informatike obvladati računalništvo, predvsem mora odlično poznati programiranje in tehnologijo prenosa podatkov ter režim dela na računalniku, v katerega nasilno posega.

Tretja in najbolj zahtevna oblika manipulacije s podatki je neupravičen poseg v računalniško evidenco preko posebnega terminala, ki ga storilec priključi na eno od komunikacijskih zvez, ki povezujejo računalnike ali terminale. Storilec mora zelo dobro poznati računalniško tehnologijo in komunikacijsko strukturo oškodovanega informacijskega sistema.

Stvarne pojavne oblike manipulacij s podatki so naslednje:

— tatvina premoženja (predmeta ali denarja) tako, da storilec v računalniški evidenci prenese podatek o nekem premoženjskem stanju s tujega računa, hranilne vloge, zavarovalne police ali drugega zapisa o premoženjskem stanju v svoj stavek;[28] to lahko stori posredno ali neposredno;[29]

— ponareditev podatkov o lastnem premoženjskem stanju, s čimer storilec pridobi premoženjsko korist (ponareditev podatkov o hranilnih vlogah, zavarovalnih policah itd.);

— ponareditev podatkov, na podlagi katerih se obračunavajo dohodki delavcev;

— izdelava ponarejenih računov in naročilnic na podlagi lažnih podatkov v računalniški evidenci;

— izdelava ponarejenih zavarovalnih polic;

[25] Najbolj pogosto uporabljeni računalniški nosilci podatkov; direktno iz formularja je možno prenašati podatke na magnetni disk samo preko terminala.

[26] Čitalec luknjanih kartic, konzola (naprava preko katere se odvija upravljalni dialog z računalnikom), lokalni terminali.

[27] Pogosto storilec strukture programov sploh ne pozna.

[28] Stavek (record) je del računalniške evidence, ki vsebuje podatke o enem subjektu, objektu, dogodku ali pojavu.

[29] Posredno: storilec izpolni vhodni formular iz katerega se prenesejo podatki v računalnik oziroma izpolni zahtevo za spremembo stanja v računalniški evidenci. Neposredno: preko terminala spremeni stanje v računalniški evidenci.

— ponareditev podatkov o opravljenih računalniških storitvah;
— ustvarjanje koristi ustanovi, organizaciji;
— prikrivanje drugega kaznivega dejanja;
— ponareditev podatkov z namenom povzročanja nelojalne konkurence.[30]

Pri ustvarjanju koristi za ustanovo gre za več pojavnih oblik. V ustanovah, organizacijah, ki so razvile ali razvijajo lastne informacijske sisteme, se večji del podatkov o financah, računovodstvu, proizvodnji, nabavi, prodaji, osnovnih sredstvih, načrtovanju in analiziranju obdeluje računalniško. Manipulacije s podatki so mnogo večje, kot so bile v klasičnem sistemu ročne ali mehanizirane obdelave. Službe, ki opravljajo nalogo vhoda in izhoda (pripravljajo vhodne in izhodne podatke) so pogosto prepričane v pravilnost svojega dela samo pri pripravi vhodnih podatkov, pri oceni izhodnih pa nemalokrat naletijo na težave. Včasih se te težave razrešijo, vedno pa tudi ne. Vzrokov za to je več in eden od njih je ta, da se v pojasnjevanje izhodnih podatkov vključijo delavci obdelave (poznavalci računalništva), pred katerimi delavec vhoda in izhoda pogosto obmolkne, ker ga ti s svojo strokovno terminologijo in razlago najbolj zapletenih postopkov »nadvladajo«. Tako se tudi zgodi, da organizacija oziroma njena služba posreduje podatke naprej, čeprav odgovorna oseba ni prepričana vanje. V takšnih razmerah nastaja dokaj ugoden položaj za tistega, ki ima namen izvesti prepovedano manipulacijo s podatki ali vplivati na tistega, ki to možnost ima. Tako se lahko prikriva dejansko finančno stanje ustanove ali organizacije, z nepravimi podatki se prikazuje neko stanje z namenom preslepitve nekoga, da sklene pogodbo itd.

Glede na to, da tudi veliko naših organizacij združenega dela uporablja računalniško obdelavo podatkov, bi morali temu vprašanju tudi pri nas posvetiti več pozornosti.

Možnih oblik **prikrivanja drugega kaznivega dejanja** s prepovedano manipulacijo podatkov je več. Odgovorna oseba ali odgovorne osebe v ustanovi, organizacij lahko s pritiskom ali dogovorom dosežejo, da se ponaredijo podatki v računalniški evidenci, s čimer se prikrije določeno kaznivo dejanje, storjeno pred tem. Druga oblika je **prikrivanje izdaje nekritih čekov.** Delavec, ki ima možnost manipulirati (bančni delavci) s podatki v računalniški evidenci, izdaja nekrite čeke in to prikrije s ponareditvijo podatkov v računalniški evidenci.

O prepovedani manipulaciji s podatki **v prid nelojalne konkurence** govorimo takrat, ko ustanova, organizacija ali privatna oseba spreminja podatke v računalniški evidenci (posredno ali neposredno) z namenom, da z njimi pridobi neko prednost pred konkurenco oziroma da to uniči. Ta dejanja so največkrat povezana z dejanji poslovnega vohunstva.

b) Neupravičen dostop do podatkov

V drugo skupino zlorab podatkov sodijo neupravičeni dostopi do podatkov, kar nekateri

[30] V veliki kanadski državni ustanovi je manipulant s podatki v avtomatski obdelavi podatkov skrbel za ažuriranje računalniške evidence o sezonskih delavcih, ki je služila za obdelavo dohodkov delavcev. Po temeljitem premisleku je izdelal naslednji načrt: v seznam novih delavcev je z enakim pisalnim strojem, s kakršnim je bil napisan seznam, ki ga je prejel od parka za zaposlovanje delavcev, vnesel še delavca z izmišljenim priimkom in veljavnim naslovom. Sprva se je nekoliko bal, da bo kontrola izmišljeni priimek odkrila, pa je hitro ugotovil, da je to pri velikem številu podatkov malo verjetno. Računalnik je za izmišljenega delavca izdelal plačilni seznam in pravilno odvedel davek. Manipulant je že pri naslednjem obračunu dohodkov črtal izmišljene podatke iz prvotnega seznama in ga vstavil v drug seznam, v drug okoliš, s čimer je preprečil večje obremenjevanje enega okoliša, kar bi lahko postalo sumljivo. Plačo izmišljenega delavca je računalnik nakazal na naslov, na katerem je ta »bival«.

Naslednji mesec je poskusil z dvema takšnima delavcema, nato s tremi. Na enem plačilnem seznamu jih je obdržal največ 3 mesece.

Manipulant je za vse izmišljene priimke in prave (dejansko obstoječe) naslove odprl bančne račune in tako tedensko dobival tudi do 3000 dolarjev. Problem pa je nastal, ko so v upravi računalniškega centra sklenili, da bodo vodjem delovišč začeli pošiljati sezname delavcev, za katere je računalnik na njihov naslov bivališča pošiljal plačilne liste. Manipulant je zadevo rešil tako, da je v svoje »podjetje« vključil še delavca, ki je razpošiljal sezname. Ta je iz njih črtal fiktivne delavce. Mirno sta živela in prejemala dokaj zajetne vsote nekaj let. Vprašanje je, kdaj bi ju odkrili, če se nekega dne ne bi delavec, ki je razpošiljal sezname, pripeljal na delo z novim dragim avtomobilom. **Vir: Alderman, s. 32.**

Neko kovinarsko podjetje iz Pforzheima v Zahodni Nemčiji je na računalniku hranilo in obdelovalo podatke o svojih dobaviteljih. Programerja, ki sta podatkovno bazo in obdelavo dobro poznala, sta v stavku dveh dobaviteljev nadomestila imeni in kombinaciji bančnih računov z ustreznimi podatki svojega lažnega podjetja. Tako je vsak predloženi račun teh dveh dobaviteljev računalnik poravnal z naročilnim čekom. Storilca sta se zavarovala tudi tako, da sta na hišo, kjer naj bi imelo sedež njuno lažno podjetje, obesila pisemski nabiralnik. Odkrili so ju slučajno, ko je bil eden od čekov nepravilno nakazan (ta napaka ni imela zveze z dejanjem programerjev) in je stekla ročna kontrola. **Vir: Das neue Verbrechen: Computerkriminalität, s. 1.**

avtorji imenujejo **tatvine podatkov,**[31] drugi pa ta dejanja uvrščajo med **računalniško vohunstvo.**[32] Gre za poskuse ali nedokončana dejanja prepovedane seznanitve s podatki, ki se hranijo na računalniških (magnetnih) medijih. Osnovni načini storitve so zelo raznoliki in odvisni tudi od stopnje razvitosti oškodovanega informacijskega sistema. V povprečju imajo ti storilci iz računalništva in informatike več znanja kot storilci prepovedanih manipulacij s podatki. Iz znane tuje kazuistike je razvidno, da je večji del računalniškega vohunstva storjenega med legalno ali nelegalno obdelavo podatkov na računalniku, ki zahteva znanje iz računalništva in uporabne informatike. Tista dejanja, ki so storjena na vhodu ali izhodu informacijskega sistema, pa zahtevajo predvsem precej znanja iz uporabne informatike. Glede na to, da mora biti za vsa dejanja, ki jih uvrščamo med kriminaliteto v zvezi z računalniki, izpolnjen osnovni pogoj,[33] ne moremo šteti med računalniško vohunstvo prepovedano seznanitev s podatki, ki jih storilec prebere na vhodnem ali izhodnem računalniškem dokumentu in pri tem ne rabi nobenega znanja iz računalništva ali informatike.

Vprašljivo je tudi uvrščanje kaznivega dejanja izdaje uradne ali poslovne tajnosti v skupino računalniškega vohunstva v primerih, ko storilec do podatkov, ki jih je izdal, ni prišel z neupravičenim posegom, ampak se z njim seznanja pri opravljanju svojega dela (programerji, delavci, ki upravljajo podatkovno bazo, neposredni uporabniki podatkov itd.). Osnovni pogoj — znanje iz računalništva in informatike — je sicer izpolnjen, toda ni prepovedanega dejanja, pri katerem bi storilec to znanje uporabil, gre za običajno izdajo tajnosti. Pri možnem obravnavanju storilca mu znanje iz računalništva in informatike ne bi šteli niti kot olajševalno niti kot obteževalno okoliščino.

Vse načine storitve, ki smo jih omenili v zvezi s prepovedano manipulacijo s podatki, razen že izvzetega vpogleda v dokumente, srečamo tudi pri neupravičenem vpogledu v podatke. To so: dostop do memoriranih podatkov preko obstoječih vhodno-izhodnih enot računalnika z obstoječo in nespremenjeno programsko opremo, preko obstoječih vhodno-izhodnih enot z obstoječo, toda prirejeno ali v ta namen izdelano programsko opremo, in preko posebne vhodno-izhodne enote, ki jo storilec priključi na eno od komunikacijskih poti, ki povezujejo računalnike in terminale. V vseh primerih je storilec več ali manj dober poznavalec računalništva in oškodovanega informacijskega sistema.

Temeljno dejanje je neupravičen dostop do podatkov, ki ga lahko spremlja še prepovedano dejanje, s katerim je storilec prišel do zaščitnega gesla ali šifre za vstop v podatkovno bazo.

Vohunstvo za računalniškimi podatki kot metoda dela raznih obveščevalnih služb je posebno poglavje, ki presega temo tega članka. Nas zanima predvsem storilec, ki je skoraj vedno delavec oškodovanega informacijskega sistema. V večini znanih tujih primerov je bil storilec računalniški strokovnjak-programer, operater na računalniku ali delavec, ki je upravljal s podatkovno bazo.

Poleg »prodajanja« podatkov pa so možni tudi primeri, ko storilec obdrži podatke zase **z namenom izsiljevanja** (z neupravičenim dostopom v računalniško podatkovno bazo izve o nekom nekaj, kar bi mu lahko škodovalo, če bi to storilec odkril drugim), in za uporabo podatkov za **opravljanje lastne dejavnosti.** Na primer: storilec, ki se ukvarja tudi s prodajo knjig, v računalniški evidenci ugotovi naslove oseb, ki razmeroma pogosto kupujejo knjige, ali ugotovi, da so tik pred tem, da odplačajo zadnji obrok naročene zbirke. Na podlagi teh informacij se »pravočasno« pojavi z novo ponudbo. Primer je zelo preprost, vendar pa so možne oblike tovrstnih dejanj s hudimi posledicami.[34]

[31] Hitha, s. 228.
[32] Zima, s. 2.
[33] Glej opombo 18.

[34] Kriminalistični uslužbenec avstrijskega notranjega ministrstva je imel preko terminala dostop do podatkov kazenskega registra in podatkov o registraciji vozil. V letih 1974—1978 si je na podlagi teh podatkov protipravno izdelal detektivsko zbirko. **Vir: Zima, s. 2.**

Leta 1976 so v ZR Nemčiji prijeli dve osebi, ki sta poskusili načrte za bojno letalo »Tornado« prodati vzhodni obveščevalni službi. To letalo je skupni izdelek ZR Nemčije, Velike Britanije in Italije. Samo ZR Nemčija je do časa storitve v ta projekt vložila 24 milijard DM. Storilca naj bi načrte dobila iz računalnika tvrdke Messerschmitt-Bölkow-Bloh, naprej pa naj bi jih prodala za 20 milijonov DM. **Vir: Zima, s. 2.**

V ZR Nemčiji so prijeli devet oseb, ki so nameravale vzhodni obveščevalni službi prodati strogo varovane informacije o IBM računalnikih, ki so jih dobili prav v teh računalnikih. **Vir: Computer Crime, Criminal Justice Resource Manual, s. 361.**

Za 50 pfenigov po osebi je neki uslužbenec elektronskega računskega centra prodal konkurenčni firmi 327 000 naslovov trgovske razpošiljalnice, v kateri je bil zaposlen (ZR Nemčija). **Vir: Das neue Verbrechen: Computerkriminalität, s. 1.**

V računalniških bazah podatkov je na **zelo majhnem prostoru zbranih veliko število podatkov.** Pri nas temu posvečamo premalo pozornosti, čeprav vemo, da je iluzorno misliti, da vedno večjemu razvoju informatike na vseh področjih kriminaliteta ne bo prizanesla. Poleg tega je Jugoslavija kot samoupravna, socialistična in neuvrščena država središče zanimanja vzhoda in zahoda. Praktično se vsak podatek po svoje razlaga in izkoristi za takšne ali drugačne pritiske na našo državo. Najbrž ni treba poudariti, da so lahko med »poklicnimi zbiralci« informacij tudi računalniški strokovnjaki.

2. Zloraba programskih postopkov in opreme

Čeprav je bila programska oprema že večkrat omenjena, ne bo odveč nekaj besed o njej.

Programsko opremo sestavljajo vsi programi, ki se uporabljajo pri upravljanju in delovanju računalniškega sistema. Program pa je zaporedje ukazov, navodil, ki posredovani računalniku sprožijo izvajanje določenih potrebnih računalniških operacij. Celotno programsko opremo (vse programe) delimo v upravljalne (sistemske) in aplikativne (uporabnikove) programe. Sistemski programi upravljajo in vodijo delo računalnika in jih običajno skupaj z računalnikom (hardwareom) prodaja proizvajalec, aplikativne programe pa je do nedavnega v največji meri izdelal uporabnik sam, v zadnjem času pa je programski trg tudi s temi programi dobro založen.

Pravila, po katerih se odvijajo vse aktivnosti informacijskega sistema, so navadno zelo obširna in stroga, kar je povsem razumljivo. Metode dela so natančno določene, kar še posebej velja za izvajanje obdelave na računalniku. V tuji in naši literaturi se uporablja angleška beseda **software,** s katero se v računalniški obdelavi podatkov označuje programska oprema in postopki — metode dela.

Zloraba programske opreme in postopkov[35] je v kriminaliteti v zvezi z računalniki močno zastopana. Gre za vse oblike dejanj, pri katerih storilci zlorabijo obstoječe programe in postopke oziroma dodajo nove z namenom, da dosežejo prepovedan cilj.

Delimo jih v:

— manipulacijo s programi,

— manipulacijo s postopki,

— neupravičeno prodajo in tatvino programov in postopkov.

a) Manipulacija s programi

Pri manipulacijah s programi gre za vse oblike spreminjanja, brisanja in prodajanja programskih ukazov ali celih programov. Bistvena razlika med prepovedano manipulacijo s podatki in prepovedano manipulacijo s programi je glede na posledice v tem, da gre v prvem primeru za enkratno posledico, v drugem pa ima **enkratna sprememba programa za posledico večkratno spreminjanje podatkov,** tolikokrat, kolikokrat se popačen program uporabi na računalniku. Zato je zloraba programov v primerjavi z zlorabo podatkov težja oblika zlorabe računalnika. Samo zaradi tega tudi obravnavamo manipulacijo programov posebej, čeprav je običajno manipulacija s programom dejansko le **pripravljalno dejanje,** ki ob pravi priložnosti omogoči izvršitev **glavnega dejanja** — ponareditev ali neupravičeno seznanitev s podatki.

Načini posegov v programsko bazo[36] so enaki načinom, ki smo jih omenili pri zlorabi podatkov, zato se bomo ustavili samo pri najvažnejših do sedaj poznanih načinih manipulacij s samimi programi.

To so:

— dodajanje fiktivnih ukazov, predvsem fiktivnih računskih operacij in fiktivnih knjiženj,

— spreminjanje računskih formul,

— spreminjanje vrednosti programskih konstant,[37]

— dodajanje fiktivnih konstant (bančni račun) in

— izločanje posameznih ukazov ali celih skupin ukazov.

Značilno za vse tovrstne manipulacije je to, da programi še vedno opravljajo svojo nalogo — obdelave tečejo dalje, toda istočasno se prikrito **odvijajo prepovedane operacije** oziroma se opuščajo nujne operacije, kar je posledica zlonamerno vgrajenih ali opuščenih programskih ukazov. Nekateri to imenujejo **metoda trojanskega konja.**[38]

Največ do sedaj znanih primerov govori o takšnih ali drugačnih oblikah okoriščanja s hra-

[35] Zloraba softwarea.

[36] Programsko bazo sestavljajo vsi memorirani programi na računalniških nosilcih podatkov in programov.

[37] Programske konstante so podatki, ki so izjemoma vključeni v program (niso v podatkovni bazi).

[38] Computer Crime, Criminal Justice Resource Manual, s. 11.

nilnimi vlogami, o prenašanju denarnih zneskov iz tujih računov na storilčev račun in okoriščanju v zvezi z dohodki dela in tujimi osebnimi dohodki. Znani pa so še primeri protipravnega pridobivanja predmetov (storilec s programom zmanjša zalogo in razliko dvigne) in sestavljanja lažnih naročil.[39]

Za opisane oblike manipulacije s programi je značilno, da storilec najbolj pogosto deluje sam, marljivo opravlja svoje redno delo in pomagača vključi le, če naleti na oviro, ki ni na dosegu njegove roke. Njegovo strokovno znanje je vedno na visoki ravni, zato ima dostop tudi do programov in podatkov, ki niso v njegovi delovni pristojnosti.

Storilci **spreminjajo predvsem aplikativne programe,** ki so jih izdelali sami in sami tudi skrbijo zanje, redko pa se lotijo sistemskega programa.

Za svoje delo lahko **prejmejo tudi plačilo.** To so primeri, ko storilci — programerji in drugi računalniški strokovnjaki — pred odhodom iz organizacije, ustanove namerno priredijo program, in to tako zapleteno, da ga njihovi nasledniki ne morejo spraviti v red. Skoraj vedno gre za programe, ki izvajajo nujne obdelave (obračun dohodka, finančno-materialno poslovanje itd.) in je lastnik, organizacija ali ustanova, pripravljen bivšemu delavcu dobro plačati, samo da vzpostavi program. Ta navadno zelo hitro odkrije napako in program dela, pogosto pa z njegovim odhodom zopet nastopijo težave. Storilci na ta način dosežejo, da se vračajo v bivšo organizacijo in še plačani so za to. Tem sicer dokaj pogostim zlorabam se vsaka organizacija, ustanova lahko izogne tako, da sta z vsakim programom do podrobnosti seznanjena vsaj dva delavca. Znane so še **naročene manipulacije s programi.** Tuja organizacija ali ustanova podkupi programerja ali drugega primernega delavca, ki za plačilo priredi program ali programe in na ta način povzroči škodo matični organizaciji. Ni nujno, da je storilec zaposlen v oškodovani organizaciji. Lahko je strokovnjak, ki ga organizacija najame kot pomoč, lahko je izurjen tehnik, ki se »poklicno« razume samo na računalniško opremo itd. Za takšnimi manipulacijami stojijo konkurenčne firme (najbolj pogosto), politične stranke in seveda tudi razne obveščevalne službe, vse skupaj pa lahko označimo za poslovno ali politično sabotažo. Storilci

[39] V ZDA je operater pri računalniku, ki je dovolj dobro poznal programiranje, vgradil v program obračunavanje obresti naslednje ukaze: pri vsakem obračunu obresti se od posameznih kontov odtegne po 1 dolar in nakaže na konto operaterja, kadar je stanje na kontu večje od 500 dolarjev, kadar ni prikazan v okroglem znesku in končno kadar se je znesek od zadnjega obračuna obresti spremenil. S temi omejitvami je operater skušal zmanjšati možnost, da bi ga odkrili. **Vir: Zima, s. 2.**

Zelo izpopolnjeno obliko prepovedane programske manipulacije je razvil v ZR Nemčiji rezervni poročnik, izšolan za poklic sistemskega analitika. V program, ki je obračunaval dohodke delavcem in izpisoval tudi plačilne ovojnice, je vgradil celo programsko rutino, ki je zanj nakazovala dodatno plačilo in izpuščal izpis »izdajalskega« obračuna — plačilne ovojnice. Zato, da bi bilo pri bilancah vse v redu, je z dodatnimi manipulacijami poskrbel, da se je znesek oddvajal od davčnih izplačil tovarne. Njegova taktika je bila tako spretna, da finančni strokovnjaki niso ničesar opazili. Programski manipulant je hitro obogatel za 192 000 mark in pobegnil. **Vir: Das neue Verebrechen: Computerkriminalität, s. 1.**

Prav tako tehtno je izpeljal svoj primer programer v veliki kanadski Narodni banki. Veljal je za enega najboljših programerjev in so mu tudi veliko zaupali. Svoje programe je lahko testiral tudi po koncu delovnega časa in preko terminala je imel direkten dostop do podatkovne in programske baze. Za svoje delo je prejemal letno 25 000 dolarjev, sčasoma pa se mu je zdelo, da je to premalo. Izdelal je načrt. V več bančnih poslovalnicah je odprl hranilne račune. Preko terminala si je iz računalniške evidence izpisal hranilne račune, na katerih je bilo vloženih najmanj po 300 dolarjev, vendar v zadnjih mesecih lastnik ni dvigal niti vlagal novih zneskov. Takšne »neaktivne« račune je izbral, ker je pričakoval, da bodo neaktivni še nekaj časa.

Z modificiranim programom je preko terminala zmanjšal vsoto na teh računih za 50 dolarjev in jih prav tako preko terminala nakazal na račune fiktivnih lastnikov (svoje račune). Transakcija je bila v redu izvedena, toda ostal je zapis na magnetnem traku. Ustanove, ki uporabljajo terminale, se zavarujejo proti neupravičenim akcijam tako, da imajo v računalniku stalno aktiven program, ki vsak poseg preko terminala zabeleži na magnetnem traku ali disku.

Dobro poučeni programer je to vedel in se na podlagi zaupanja, ki ga je užival, dokopal tudi do programa, s katerim je lahko »prečistil« omenjeni trak.

Od 50 dolarjev je prišel na 75, nato na 100, nikoli pa na vrednost, ki bi lahko vzbudila sum. Na bankah je mirno dvigal denar iz svojih hranilnih vlog, vendar pa ni dolgo obdržal računa v eni banki. Po določenem času ga je izčrpal, zaprl in odprl v drugi podružnici, se vsedel za terminal in ga »napolnil«.

Po določenem času se je nabralo toliko pritožb lastnikov, da je stekla preiskava, ki je bila zelo dolgotrajna in draga. Dejanski zaključek preiskave ni znan. **Vir: Alderman, s. 34.**

Organizirani južnokorejski in ameriški »strokovnjaki« so z manipulacijo programov in podatkov na računalniku ameriške vojske v Južni Koreji oškodovali ameriško vojsko za več kot 10 milijonov dolarjev letno. **Vir: Bequai, Organized Crime in the Computer Arena, s. 26.**

po naročilu program modificirajo zato, da z njim ponaredijo podatke med izvajanjem programa, ali pa pokvarijo program tako, da ga ni mogoče uporabiti, in na ta način povzročijo škodo.

Kot zadnje pa omenjamo prepovedane manipulacije s programi, ki jih storilci izvedejo zaradi **maščevanja, užaljenosti, škodoželjnosti in podobnih nagibov.** Odpuščeni računalniški delavci so možni storilci takšnih dejanj. Zaradi odhoda iz organizacije, zaradi spora z vodilnimi delavci ali tudi zaradi škodoželjnosti, da bi povzročil škodo, se maščeval delovnemu tovarišu itd., namerno priredi program. Najbolj znana pojavna oblika takšnih dejanj so **logične bombe.**[40] To je programska rutina ali nekaj posameznih ukazov, ki so zelo skrito vstavljeni v program in se izvedejo **ob natančno določenem času,** njihova izvedba pa ima škodljive posledice. Ko »logična bomba eksplodira«, je storilec lahko že zelo daleč, ustanova je nanj že zdavnaj pozabila. V program se vstavi po metodi trojanskega konja. To je zelo nevarna oblika zlorabe programov, še zlasti zato, ker organizacija ali ustanova po nekaj mesecih odhoda delavca ni več pozorna na njegovo zapuščino.[41]

Večji del prepovedanih manipulacij je **odkritih slučajno.** Poudariti je treba, da ima storilec po odkritju na voljo veliko možnosti, da »dokaže«, da gre za običajno nenamerno napako, ki jo bo hitro odpravil. To je predvsem posledica neznanja preiskovalcev in pogosto tudi interes oškodovane organizacije ali ustanove, da gre vsa zadeva čim bolj neopazno mimo.

b) Manipulacije s postopki

V literaturi skoraj ne zasledimo obravnavanja tovrstnih prepovedanih dejanj, čeprav so mogoča in imajo lahko prav tako hude posledice kot manipulacije s podatki in programi. Gre za vse oblike **spreminjanja, dodajanja ali opuščanja določenih postopkov,** ki imajo za posledico ponarejene podatke. Najhujše posledice bi povzročila dejanja manipulacije s postopki pri obdelavah na računalniku. Operater pri računalniku, ki dobro pozna svoje delo in določene obdelave, lahko zamenja vrstni red izvajanja dveh ali več programov, s čimer povzroči nepravilno spremembo v podatkovni bazi. Pri večini obdelav se vrstni red izvajanja programov sicer avtomatsko nadzoruje, vedno pa to ni mogoče.

Možnosti za manipulacijo s postopki so v vseh štirih skupinah dejavnosti informacijskega sistema — na vhodu, izhodu, med obdelavo in pri vzdrževanju povratne veze.

c) Neupravičena prodaja in tatvina programov in postopkov

O dejanjih neupravičene prodaje programov in postopkov govorimo takrat, ko storilec-programer, sistemski analitik, operater ali drug računalniški delavec — proda program ali postopek, ki ga je izdelal med opravljanjem rednega dela za organizacijo, v kateri je zaposlen, in je za to prejel redni dohodek ter nima od svoje organizacije nobenega pooblastila za prodajo. Kupec je običajno organizacija sorodne dejavnosti, ki na ta način poceni pride do programskih in organizacijskih — postopkovnih rešitev. Takšna neupravičena prodaja je bila bolj razširjena v času, ko odprti programski trg še ni bil tako razvit, kot je danes, ko je možno velik del aplikativne programske opreme legalno kupiti oziroma najeti. Preganjanje storilca se je zanj skoraj vedno uspešno končalo, kar je zlasti zaradi pomanjkljivih predpisov težko dokazati, da je prodal ravno tisti program, ki ga je izdelal med opravljanjem svojega dela, popolno podporo pa je imel v kupcu.

Storilec je izvirni program prepisal z magnetnega traku, magnetnega diska ali luknjanih kartic na drug magnetni trak, ki ga je v ta namen dobil od kupca, ali pa je izvirnik na traku ali karticah skrivoma odnesel iz matične organizacije, ga drugje prepisal in vrnil. Pri tem je izrabil svoj položaj, prestopil meje svojih pravic z namenom, da sebi pridobi protipravno premoženjsko korist.

Tatvine programov in postopkov se od neupravičene prodaje razlikujejo v tem, da storilec program ali postopek (na papirju, magnetnem traku, magnetnem disku, luknjanih karticah, mikrofilmu, filmu) ukrade in ga ne samo prepiše. Da dejanje štejemo med kriminaliteto v zvezi z računalniki, mora biti izpolnjen osnovni po-

[40] Computer Crime, Criminal Justice Resource Manual, s. 21.

[41] V ZDA je programer vstavil v program, ki je obdeloval osebno evidenco, rutino, ki bi v celoti izbrisala evidenco, če bi nekdo iz nje črtal njegov priimek. **Vir: Computer Crime, Criminal Justice Resource Manual, s. 366.**

Drugi primer govori o delavcu, ki je zaradi maščevanja organizaciji, iz katere je bil odpuščen, pred odpustom vstavil v program rutino, ki se je »sprožila« šele po njegovem odhodu. Točno po 2 letih, ob 3. uri popoldan so se na vseh 300 terminalih pojavili zaupni podatki, nato pa je celoten računalniški sistem izpadel. **Vir: Computer Crime, Criminal Justice Resource Manual, s. 367.**

goj, v nasprotnem primeru gre za običajno tatvino.

Neupravičena prodaja in tatvina programov in postopkov je nedvomno nevarna oblika kriminalitete v zvezi z računalniki, s težkimi posledicami za oškodovano organizacijo, vendar pa jo je možno z učinkovitim sistemom zaščite in nadzora ter njegovim doslednim upoštevanjem zmanjšati na minimum.

3. Neupravičena uporaba računalniške in programske opreme

V tretjo skupino zlorab računalnika spadajo neupravičene uporabe računalnika in programov. Takoj pa je treba dodati, da je možna in tudi v praksi najbrž že izvedena neupravičena uporaba dela baze podatkov, čeprav pa pri tem ne gre niti za pravo prepovedano manipulacijo s podatki niti za neupravičen dostop do podatkov (računalniške evidence naselij, ulic, cest, občin, krajevnih skupnosti itd.). Med neupravičeno uporabo uvrščamo vse primere uporabe računalnika, programov in podatkov organizacije ali ustanove, v kateri je storilec zaposlen oziroma druge organizacije ali ustanove, v katero lahko storilec legalno vstopi.

Največkrat gre za neupravičeno uporabo računalnika — tatvino računalniškega časa.[42] Storilec med ali izven rednega delovnega časa izvaja na računalniku programe, ki jih je sam izdelal ali od kje prinesel, rezultati obdelave so namenjeni drugi organizaciji ali ustanovi, za to delo pa storilec nima nobenega dovoljenja ali pooblastila od organizacije ali ustanove, katere last je računalnik. Izhaja skoraj vedno iz vrst računalniških delavcev, najbolj pogosto iz vrst programerjev ali sistemskih analitikov. Čeprav govorimo ločeno o neupravičeni uporabi računalnika in neupravičeni uporabi programov, pa je prvo brez druge skoraj nemogoče izvesti. Čim nekdo uporablja računalnik, uporablja istočasno sistemsko programsko opremo, ki sploh omogoča delovanje računalnika; kar pa se jemlje kot nekaj, kar je samo po sebi umevno. Med neupravičeno uporabo programov se v praksi šteje le **neupravičena uporaba aplikativnih programov.** Storilec prinese s seboj na magnetnem mediju podatke, ki jih z uporabo aplikativnega programa obdela in rezultate zopet odnese.

Neupravičena uporaba programov in predvsem računalnika je najbrž pogosta praksa zlasti v manj razvitih informacijskih sistemih, kjer še ni avtomatske kontrole vseh obdelav, ki se izvajajo na računalniku. Nekateri informacijski sistemi so tej problematiki posvetili veliko pozornosti in računalnik na poseben magnetni trak ali disk zapisuje podatke o vseh programih, ki se izvajajo, šifre programerjev, imena računalniških evidenc, v katere posegajo programi itd. Na podlagi takega protokola je razmeroma lahko ugotoviti neupravičeno delo in ga tudi preprečiti.[43]

Pri neupravičeni uporabi omenjamo še dejanja, pri katerih se računalnik uporablja za **načrtovanje, simulacijo in vodenje kriminalnih dejanj.** Gre za najvišjo obliko zlorabe računalnika.[44] Organiziran kriminal naroči delo »sodelavski« ustanovi, lahko pa ima lasten računalnik, da z uporabo najsodobnejših matematičnih, informativnih in kibernetskih metod pripravi najboljšo varianto izvedbe kaznivega dejanja. Računalnik v nekaj sekundah, morda minutah najde optimalno rešitev, pri čemer upošteva vse možne okoliščine, čas storitve dejanja, razporejene policijske sile, oddaljenost kraja dejanja od najbližje policijske postaje itd. Čeprav ne gre v prejšnjem pomenu za neupravičeno uporabo računalnika, pa gre za uporabo, ki je mnogo bolj zastrašujoča kakor katerakoli druga oblika kriminalitete v zvezi z računalniki.

III. SKLEP

Kriminaliteta v zvezi z računalniki postaja v tehnološko razvitem svetu problem št. 1. Strah, da bi v prihodnosti zasenčila vse dosedanje oblike klasične kriminalitete, je najbrž upravičen. Kazniva dejanja s tragičnimi posledicami in ogromno škodo se rojevajo v množici ultraminiaturnih vezij, kar je vse skupaj za povprečnega človeka nerazumljivo in nihče ne more od njega niti zahtevati, da bi to razumel. To so kazniva dejanja, pri katerih »ni dima, ni glasu, ni ranjenih žrtev«,[45] ni ničesar, kar bi preiskovalcu padlo v oči. Izvršeni so v delčkih sekunde.

[42] Das neue Verbrechen: Computerkriminalität, s. 1.

[43] V ZDA je nek ameriški projektivni biro s 50 inženirji uporabljal računalnik za izdelavo načrtov. 16 inženirjev pa je dalj časa uporabljalo računalnik tudi za »dopolnilni« zaslužek, ki je ob odkritju znašal že 2,8 milijona dolarjev. Do prijave sploh ni prišlo, ker so se s firmo dogovorili, da škodo povrnejo **Vir: Zima, s. 3.**

[44] Computer Crime, Expert Witness Manual, s. 4.

[45] Prav tam.

Uporaba računalnikov pa narašča. V ZDA je več kot 90 000 računalnikov, s katerimi upravlja preko 2 milijona ljudi.[46] Ni ameriškega državljana, ki ne bi bil na tak ali drugačen način odvisen od računalnika; podobno je v vseh razvitih državah. In pri nas?

Počasi, toda vztrajno se opremljamo z računalniki. Imamo jih prek 2000. Po poročilih Zveznega zavoda za statistiko iz leta 1978 je bilo v Jugoslaviji pri uporabi računalnikov zaposlenih nekaj več kot 17 000 ljudi. Tudi kriminaliteta v zvezi z računalniki se že pojavlja. Odkritih je bilo nekaj primerov vseh pojavnih oblik zlorabe računalnikov. Toda ne moremo reči, da ni zlorab še več, najbrž je temno polje večje od svetlega. Organi za notranje zadeve sicer že imajo nekaj strokovnjakov, ki so usposobljeni za raziskovanje zlorab računalnikov, nimamo pa izdelanih metod za njihovo zaznavanje — odkrivanje. Tako kot drugod po svetu še vedno prevladuje naključje. Prej ali slej bo morala o tem nekaj reči tudi kazenska zakonodaja.

Pri dejanjih zlorabe računalnikov ugotavljamo nekaj značilnosti, ki jih pri drugih kaznivih dejanjih ne zasledimo ali so manj izrazite.

1. Povzročena škoda je zelo velika, storilec pa razmeroma zelo hitro, brez večjega truda izvede kaznivo dejanje. V študiji nekaj sto primerov zlorab računalnikov je ugotovljena povprečna škoda 400 000 dolarjev.

2. Žrtev dejanja, največkrat pravna oseba, z odporom sodeluje pri raziskavi dejanja, predvsem iz strahu, da izgubi poslovno zaupanje. Na splošno lahko rečemo, da je sodelovanje žrtev minimalno.

3. Zlorabe računalnikov niso vidna dejanja in zato jih tudi zelo težko odkrivamo.

4. Zloraba računalnika je dejanje, ki ga je možno izvesti na daljavo. Storilec je lahko na drugi celini in preko terminala izvede dejanje v računalniku, ki je nekaj tisoč kilometrov oddaljen od tega (velike možnosti za organiziran mednarodni kriminal).

5. Storilci izvedejo dejanja z uporabo svojega znanja, ki ga ima zelo malo ljudi, in so toliko bolj prepričani v svoj uspeh. Dejanja izvršujejo z veliko psihološko gotovostjo. K temu je brez dvoma pripomogla tudi neupravičena »glorifikacija« računalnika v preteklih letih.

6. Storilci imajo v povprečju vsi najmanj srednjo izobrazbo, veliko jih je pa z višjo ali visoko izobrazbo.

7. Protipravna premoženjska korist ni vedno edini motiv zlorabe računalnika. Do sedaj znani tuji primeri so pokazali, da gre storilcu pogosto za to, da »premaga« računalnik, da pokaže svoje sposobnosti tako, da pride do podatkov, ki so pod okriljem fizične, programske in še kakšne zaščite.

8. Razčlemba kaznivega dejanja zlorabe računalnika na elemente in modus operandi delata večini preiskovalcev težave.

9. Natančnega časa storitve kaznivega dejanja pogosto ni mogoče ugotoviti. Pripomniti je treba, da se dejanje, ki ima za posledico ogromno škodo, lahko izvede v nekaj tisočinkah sekunde.

10. Preiskovalci lahko raziskujejo in analizirajo le podatke in programe, izpisane na papirju, mikrofilmu, filmu ali prek terminala, saj ni mogoče ničesar razbrati neposredno na magnetnem traku ali disku. Če hočejo biti povsem gotovi, da je izpis popolnoma verodostojen, ga morajo izdelati z lastnim programom.

Pred odkrivanjem in raziskovanjem kriminalitete v zvezi z računalniki ima vso prednost preprečevalno delovanje. Z njim se v svetu ukvarja veliko znanstvenikov in računalniških strokovnjakov. V zaščito informacijskih sistemov pred napadi tako od zunaj kot od znotraj tudi pri nas vlagamo precej naporov, čas pa bo pokazal, če ti napori zadostujejo.

[46] Prav tam, s. 10.

LITERATURA

1. Alderman, Tom: Computer Crime, **Journal of Systems Management,** 1977, 1, s. 32—35.
2. Bequai, August: **Computer Crime,** Lexington Books, D. C. Heath and Company Lexington, Massachusetts, Toronto, Second Printing, 1978, 207 s.
3. Bequai, August: Organized Crime in the Computer Arena, **The Police Chief,** 45, 1978, 9, s. 24—29.
4. Computer Crime, **Criminal Justice Resource Manual,** Nation Criminal Justice Information and Statistics Service Law Enforcement Assistance Administration, U. S. Departement of Justice, Washington 1979, 392 s.
5. Computer Crime, **Expert Witness Manual,** U. S. Departement of Justice, Washington 1980, 120 s.
6. Computer Crime, **Legislative Resource Manual,** U. S. Departement of Justice, Washington 1980, 90 s.
7. Das neue Verbrechen: Computerkriminalität, **Der Spiegel,** 1979, 4
8. Ferišak, Vilim, in drugi: **Osnove informatike,** Informator Zagreb, Zagreb 1981, 357 s
9. Hytha, Robert: EDV Kriminalität oder Computer Schutz, Kriminalistik, 29, 1975, 5, s. 227—230.

10. Pečar Janez: Futurologija in obravnavanje kriminalnosti, **Revija za kriminalistiko in kriminologijo,** 21, 1970, 4, s. 253—264.
11. Savič, Jalov: Zaštita avtomatizovanih informacionih sistema i kompjuterski kriminalitet, **Bezbednost,** 23, 1981, s. 411—417.
12. Srića, Velimir: Informacijski sistem, Informator Zagreb, Zagreb 1978, 162 s.
13. Tomeski, Edward, in Lazaraus, Harold: **People-oriented Computer Systems,** Van Nostrand Reinhold Company, London 1975, 300 s.
14. Virant, Jernej: Opredelitev informatike in njen razvoj doma in na tujem, **Obveščanje in odločanje,** posebna številka 1981, s. 5—8.
15. Zima, Herbert: Computer — Objekt und Mittel kriminellen Handelns, **Öffentliche Sicherheit,** 45, 1980. 1, s. 1—4.

UDC 343.3/.7:681.3

Forms of Computer Abuse

Brvar, Bogo, Graduate in Mathematics and Physics, Police College, Ljubljana

The introductory part of the article summarizes definitions of computer processing, of informatics and the information system which the author relates to the definition of computer crime, this being regarded as crime in which a computer is used as a device, as the subject or object of attack. The notion of computer crime seems inconvenient to the author and he foresees that it will be replaced in the future by the expression crime in informatics.

The main part of the article is devoted to computer abuses which are divided into three principal groups: manipulations with data, manipulations with programs and processings and unauthorised use of computer and program equipment. It is stated that in all cases the modus operandi shows great heterogeneity (variety) and that the perpetrators are able to commit offences during all the four groups of activities performed by the information system: at the input, at the output, during data processing and in the frame of the feedback.

In conclusion the author gives descriptions of certain characteristics typical of computer abuse and which are not perceived in other criminal offences or are not emphasized.